

(51)Int.Cl.⁷ 識別記号 F I テーマコード* (参考)
G 0 6 F 17/60 3 0 2 G 0 6 F 17/60 3 0 2 E
G 1 0 K 15/02 G 1 0 K 15/02

審査請求 未請求 請求項の数6 O L (全 32 頁)

(21)出願番号 特願2000-326125(P2000-326125)
(22)出願日 平成12年10月25日(2000. 10. 25)
(31)優先権主張番号 特願平11-303138
(32)優先日 平成11年10月25日(1999. 10. 25)
(33)優先権主張国 日本 (J P)

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川 6 丁目 7 番35号
(72)発明者 石黒 隆二
東京都品川区北品川 6 丁目 7 番35号 ソニ
ー株式会社内
(72)発明者 河上 達
東京都品川区北品川 6 丁目 7 番35号 ソニ
ー株式会社内
(74)代理人 100067736
弁理士 小池 晃 (外2名)

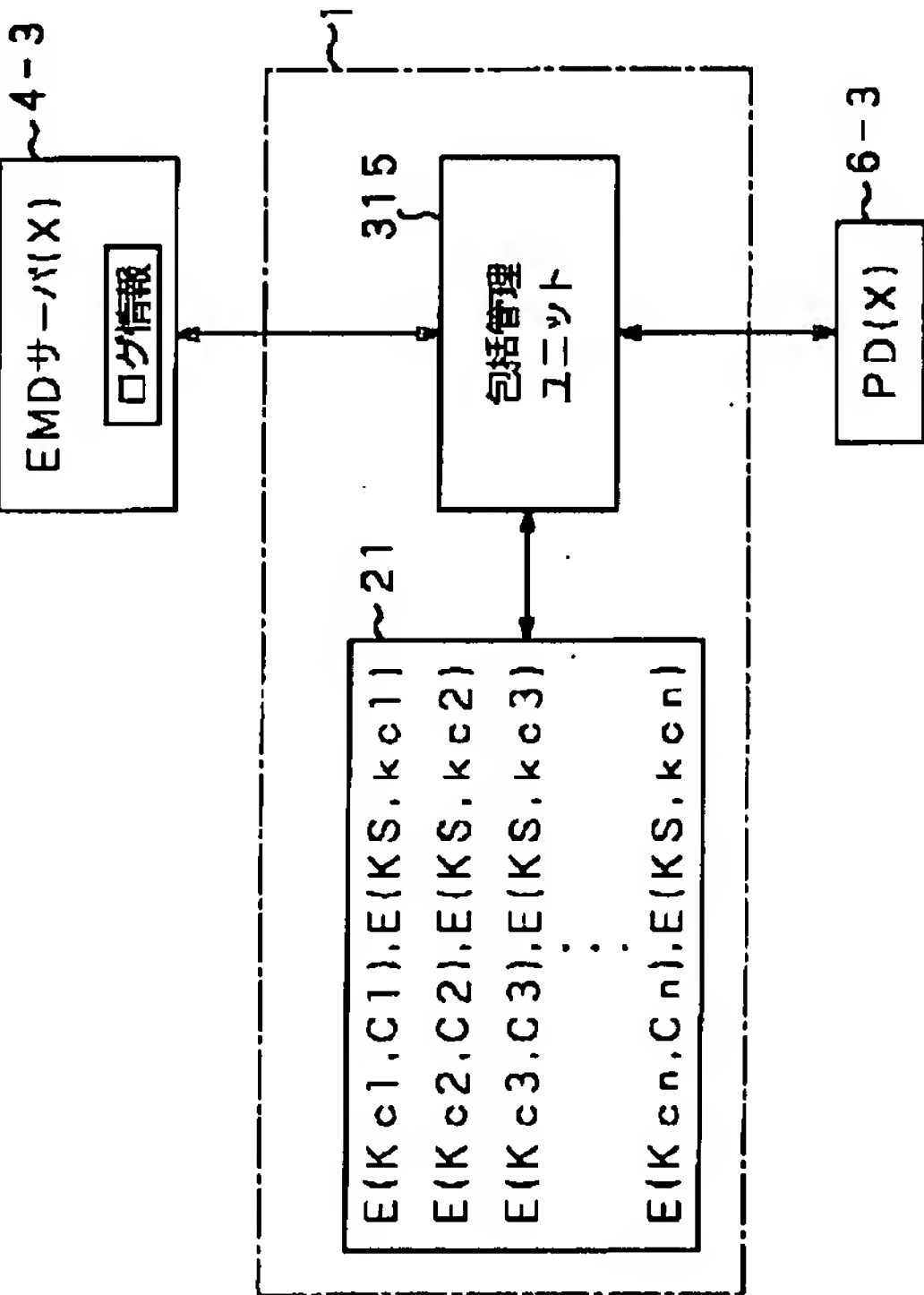
最終頁に続く

(54)【発明の名称】 コンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体

(57)【要約】

【課題】 ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元する。

【解決手段】 P Cは、配信された音楽コンテンツのバックアップをハードディスクに記憶するとともに、ハードディスクに格納している音楽コンテンツの使用ログ情報をE M Dサーバに送信する。P Cは、例えばハードディスク内の音楽コンテンツが破壊したときには、使用ログ情報をE M Dサーバから取得し、使用ログ情報に応じてハードディスクに記憶しているバックアップデータの再生をする。



【特許請求の範囲】

【請求項1】 コンテンツデータをネットワークを介して配信するコンテンツサーバと、
コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とするコンテンツ提供システム。

【請求項2】 コンテンツデータをネットワークを介して配信するコンテンツサーバと、
コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とするコンテンツ提供システム。

【請求項3】 コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、
コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、
上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、
上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアッ

プデータの再生及び／又は制御をすることを特徴とするコンテンツ配信方法。

【請求項4】 コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、
コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、
上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、
上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とするコンテンツ配信方法。

【請求項5】 データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
上記再生制御プログラムは、
上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする記憶媒体。

【請求項6】 データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
上記再生制御プログラムは、
上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータ

を上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを介して音楽データ等のコンテンツデータを提供するコンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体に関するものである。

【0002】

【従来の技術】近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオンライン配信が実用化され始めた。

【0003】このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Web上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するWeb等にアクセスをして、所望の音楽コンテンツをダウンロードする。

【0004】

【発明が解決しようとする課題】ところで、このような音楽配信システムにおいては、一般に、ダウンロードした音楽コンテンツに対して例えばネットワークを介して課金がされる。

【0005】しかしながら、例えば、ユーザが保有するパーソナルコンピュータ内のデータが破壊してしまうと、一旦購入した音楽コンテンツも消滅してしまう。そのため、その音楽コンテンツを復元させるには、再度、コンテンツを購入しなければならなかった。

【0006】本発明は、このような実情を鑑みてなされたものであり、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができるコンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明にかかるコンテンツ提供システムは、コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装

置とを備え、上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【0008】コンテンツ提供システムでは、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行う。

【0009】本発明にかかるコンテンツ提供システムでは、コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【0010】このコンテンツ提供システムでは、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行う。

【0011】本発明にかかるコンテンツ配信方法は、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【0012】このコンテンツ配信方法では、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は

制御を行う。

【0013】本発明にかかるコンテンツ配信方法は、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【0014】このコンテンツ配信方法では、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行う。

【0015】本発明にかかる記憶媒体は、データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、上記再生制御プログラムは、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【0016】この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行わせる。

【0017】本発明にかかる記憶媒体は、データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、上記再生制御プログラムは、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上

記コンテンツサーバに送信し、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【0018】この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行わせる。

【0019】

【発明の実施の形態】以下、本発明の最良の実施の形態として、本発明を適用した音楽コンテンツ配信システムについて図面を参照しながら詳細に説明する。この音楽コンテンツ配信システムは、ネットワークを介してサーバからパーソナルコンピュータやポータブルデバイスにダウンロードし、さらに、ダウンロードした音楽コンテンツやCDから読みとった音楽コンテンツの管理等を行うシステムである。

【0020】(1) 音楽コンテンツ配信システムの全体構成

図1は、本発明を適用した音楽コンテンツ配信システムの全体構成を示す図である。

【0021】この音楽コンテンツ配信システムは、パーソナルコンピュータ1と、インターネットやローカルエリアネットワーク等のネットワーク2と、登録サーバ3と、音楽データ（以下、コンテンツと呼ぶ。）を配信する複数のEMD（Electrical Music Distribution）サーバ4（4-1，4-2，4-3）と、WWWサーバ5（5-1，5-2）とを備えて構成される。また、パーソナルコンピュータ1には、USBケーブル7（7-1，7-2，7-3）を介して、内部にメモリーカード等の記憶媒体が格納され、コンテンツの再生を行う携帯型の音楽再生器機であるポータブルデバイス6（6-1，6-2，6-3）が接続される。

【0022】パーソナルコンピュータ1は、ネットワーク2を介して、EMD登録サーバ3、EMDサーバ4（4-1，4-2，4-3）、WWW（World Wide Web）サーバ5（5-1，5-2）と接続される。

【0023】パーソナルコンピュータ1は、EMDサーバ4（4-1，4-2，4-3）から、所定の圧縮方式で圧縮されたコンテンツを受信し、所定の暗号化方式で暗号化して記録する。また、パーソナルコンピュータ1は、CD（Compact Disc）等から読みとったコンテンツを、所定の圧縮方式で圧縮して、所定の暗号化方式で暗号化して記録する。圧縮方式としては、例えばATRAC（Adaptive Transform Acoustic Coding）3（商標）やMP3（MPEG Audio Layer -3）等の方式が用い

られる。また、暗号化方式としては、DES (Data Encryption Standard) などが用いられる。

【0024】また、パーソナルコンピュータ1は、コンテンツの配信を受ける場合には、そのコンテンツの利用条件を示す利用条件情報の配信も受け、それを記録する。また、パーソナルコンピュータ1は、CD等から読みとったコンテンツを記録する場合には、そのコンテンツの再生条件に応じて、利用条件情報を生成して、それを記録する。

【0025】また、パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、利用条件情報及び曲名や演奏者等の関連情報とともに、USBケーブル7 (7-1, 7-2, 7-3) を介して、ポータブルデバイス6 (6-1, 6-2, 6-3) に記録し、記憶させたことに対応して利用条件情報を更新する。この処理のことをチェックアウトという。利用条件情報は、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツのチェックアウト可能回数を1減少させる。チェックアウト可能回数が0のときには、対応するコンテンツは、チェックアウトすることができない。

【0026】また、パーソナルコンピュータ1は、USBケーブル7 (7-1, 7-2, 7-3) を介して、ポータブルデバイス6 (6-1, 6-2, 6-3) に記憶されているコンテンツを、消去し (または、使用できなくさせ)、消去したことに対応させて利用条件情報を更新する。この消去処理のことをチェックインと呼ぶ。チェックインしたとき、パーソナルコンピュータ1が記録している、そのコンテンツのチェックアウト可能回数を1増加させる。

【0027】なお、パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6にチェックアウトしたコンテンツに対してはチェックインはできない。すなわち、パーソナルコンピュータ1自身がチェックアウトしたコンテンツしか、チェックインをすることができない。

【0028】EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4 (4-1, 4-2, 4-3) からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4 (4-1, 4-2, 4-3) との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4 (4-1, 4-2, 4-3) に接続するためのプログラムをパーソナルコンピュータ1に送信する。

【0029】EMDサーバ4 (4-1, 4-2, 4-3) は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、利用条件情報及びコンテンツの関連データ (例えば、曲名、又は演奏者など) とともに、パーソナルコンピュータ1にコンテンツを供給す

る。

【0030】各EMDサーバ4 (4-1, 4-2, 4-3) が配信するコンテンツは、所定の圧縮の方式で圧縮されている。その圧縮方式は、サーバ毎に異なってもよい。また、各EMDサーバ4 (4-1, 4-2, 4-3) が供給するコンテンツは、所定の暗号化方式で暗号化されて配信される。その暗号化方式は、サーバ毎に異なってもよい。

【0031】WWWサーバ5 (5-1, 5-2) は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD (例えば、CDのアルバム名、又はCDの販売会社など) 及びCDから読み取ったコンテンツに対応するデータ (例えば、曲名、又は作曲者名など) をパーソナルコンピュータ1に供給する。

【0032】ポータブルデバイス6 (6-1, 6-2, 6-3) は、パーソナルコンピュータ1から供給されたコンテンツ (すなわち、チェックアウトされたコンテンツ) を再生し、図示せぬヘッドフォンなどに出力する装置である。

【0033】各ポータブルデバイス6 (6-1, 6-2, 6-3) は、コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なICメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス6 (6-1, 6-2, 6-3) は、USB等の物理的なインターフェース7 (7-1, 7-2, 7-3) を介してパーソナルコンピュータ1と接続され、コンテンツが転送される。このとき、コンテンツは、暗号化及び圧縮された状態で転送され、利用条件情報も付加されている。

【0034】各ポータブルデバイス6 (6-1, 6-2, 6-3) は、通常、パーソナルコンピュータ1との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化したコンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス6 (6-1, 6-2, 6-3) は、各コンテンツに付加されている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。

【0035】以下、ポータブルデバイス6-1, 6-2, 6-3を個々に区別する必要がないとき、単にポータブルデバイス6と称する。

【0036】つぎに、図2を参照して、パーソナルコンピュータ1の構成について説明をする。

【0037】CPU (Central Processing Unit) 11は、各種アプリケーションプログラム (詳細については後述する。) や、OS (Operating System) を実際に実行する。ROM (Read-only Memory) 12は、一般的には、CPU11が使用するプログラムや演算用

のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 13は、CPU 11の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス14により相互に接続されている。

【0038】ホストバス14は、ブリッジ15を介して、PCI (Peripheral Component Interconnect / Interface) バスなどの外部バス16に接続されている。

【0039】キーボード18は、CPU 11に各種の指令を入力するとき、使用者により操作される。マウス19は、ディスプレイ20の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ20は、液晶表示装置又はCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21は、ハードディスクを駆動し、それらにCPU 11によって実行するプログラムや情報を記録又は再生させる。

【0040】ドライブ22は、装着されている磁気ディスク41、光ディスク42 (CDを含む)、光磁気ディスク43、又は半導体メモリ44に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース17、外部バス16、ブリッジ15及びホストバス14を介して接続されているRAM 13に供給する。

【0041】USBポート23 (23-1, 23-2, 23-3) には、USBケーブル7 (7-1, 7-2, 7-3) を介して、ポータブルデバイス6 (6-1, 6-2, 6-3) が接続される。USBポート23は、インターフェース17、外部バス16、ブリッジ15、又はホストバス14を介して、HDD 21、CPU 11、又はRAM 13から供給されたデータ (例えば、コンテンツ又はポータブルデバイス6のコマンドなどを含む) をポータブルデバイス6 (6-1, 6-2, 6-3) に出力する。

【0042】IEC (International Electrotechnical Commission) 60958端子24aを有する音声入出力インタフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ45は、音声入出力インタフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【0043】これらのキーボード18、マウス19、ディスプレイ20、HDD 21、ドライブ22、USBポート23、音声入出力インタフェース24は、インターフェース17に接続されており、インターフェース17は、外部バス16、ブリッジ15及びホストバス14を介してCPU 11に接続されている。

【0044】通信部25は、ネットワーク2が接続さ

れ、CPU 11、又はHDD 21から供給されたデータ (例えば、登録の要求、又はコンテンツの送信要求など) を、所定の方式の packets に格納して、ネットワーク2を介して、送信するとともに、ネットワーク2を介して、受信した packets に格納されているデータ (例えば、認証鍵、又はコンテンツなど) をCPU 11、RAM 13、又はHDD 21に出力する。

【0045】半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ26のCPU 32は、外部バス16、ブリッジ15及びホストバス14を介してパーソナルコンピュータ1のCPU 11と共働し、各種の処理を実行する。RAM 33は、CPU 32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM 36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35は、計時動作を実行し、時刻情報を提供する。半導体ICは、セキュアな環境に設計されており、外部からの悪意なアクセスに対して耐性をもっている。なお、この機能は、ソフトウェアプログラムで構成されていてもよい。

【0046】通信部25及びアダプタ26は、外部バス16、ブリッジ15及びホストバス14を介してCPU 11に接続されている。

【0047】次に、図3を参照して、ポータブルデバイス6の構成を説明する。

【0048】電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU 53～表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

【0049】USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1から転送されたコンテンツを含むデータを、内部バス58を介して、CPU 53に供給する。

【0050】パーソナルコンピュータ1から転送されるデータは、1 packet 当たり64バイトのデータから構成され、12 Mbit/sec の転送レートでパーソナルコンピュータ1から転送される。

【0051】ポータブルデバイス6に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されているとともに、再生制限処理等に必要な利用条件情報等が格納されている。コンテンツは、ATRAC3などの符号化方式で符号化され、暗号化されている。

【0052】ヘッダサイズは、ヘッダのデータ長 (例え

ば、33バイトなど)を表し、ファイルサイズは、コンテンツのデータ長(例えば、33, 636, 138バイトなど)を表す。

【0053】コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ1とポータブルデバイス6との相互認証の処理で生成されたセッション鍵(一時鍵)を基に暗号化された状態で、パーソナルコンピュータ1からポータブルデバイス6に送信される。

【0054】ポータブルデバイス6がUSBケーブル7を介してパーソナルコンピュータ1のUSBポート23に接続されたとき、ポータブルデバイス6とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス6のDSP59は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読(復号)の処理を実行する。

【0055】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ1が生成するある値(チャレンジ)に対して、ポータブルデバイス6がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値(レスポンス)で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ1が生成する値は認証の処理毎に毎回変化するもので、例えば、ポータブルデバイス6が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ1は不正を検出できる。

【0056】コンテンツIDは、コンテンツに対応した、コンテンツを特定するためのIDである。

【0057】コーデックIDは、コンテンツの符号化方式に対応したIDであり、例えば、コーデックID"1"は、ATRAC3に対応し、コーデックID"0"は、MP3(MPEG(Moving Picture Experts Group) Audio Layer-3)に対応する。

【0058】ファイル名は、コンテンツに対応するパーソナルコンピュータ1が記録しているコンテンツファイル(後述する)をASCII(American National Standard Code for Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などをASCIIコードに変換したデータである。

【0059】ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツとともにコンテンツの書き込み命令を受信した場合、RAM54又はROM55から読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませ

る。

【0060】フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【0061】なお、フラッシュメモリ61は、ポータブルデバイス6にメモリカードとして着脱可能とすることができるようにもよい。

【0062】使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードとコンテンツとを読み出させ、DSP59に転送させる。

【0063】DSP59は、フラッシュメモリ61から転送された再生用コードに基づいてコンテンツをCRC(Cyclic Redundancy Check)方式で誤り検出をした後、再生して、再生したデータ(図3中においてD1で示す)をデジタル/アナログ変換回路63に供給する。

【0064】DSP59は、内部に設けられた発信回路とともに一体に構成され、外付けされた水晶で成る発振子59AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びに、フレーム単位のLチャンネルクロックLCLK及びRチャンネルクロックRCLKからなる動作クロックLRCLKをデジタルアナログ変換回路63に供給する。

【0065】DSP59は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路63に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、デジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

【0066】同様に、CPU53及びUSBコントローラ57も、水晶でなる発振子53A又は57Aがそれぞれ外付けされ、発振子53A又は57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

【0067】このように構成することで、ポータブルデバイス6は、CPU53、DSP59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

【0068】デジタルアナログ変換回路63は、再生したコンテンツをアナログの音声信号に変換して、これ

を増幅回路64に供給する。増幅回路64は、音声信号を増幅して、ヘッドフォンジャック65を介して、ヘッドフォンに音声信号を供給する。

【0069】このように、ポータブルデバイス6は、再生/停止ボタンが押圧操作されたとき、CPU53の制御に基づいてフラッシュメモリ61に記憶されているコンテンツを再生するとともに、再生中に再生/停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【0070】ポータブルデバイス6は、停止後に再度再生/停止ボタンが押圧操作されたとき、CPU53の制御に基づいて停止した位置からコンテンツの再生を再開する。再生/停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス6は、自動的に電源をオフして消費電力を低減する。

【0071】因みに、ポータブルデバイス6は、電源がオフになった後に再生/停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1曲目から再生する。

【0072】また、ポータブルデバイス6のCPU53は、LCDコントローラ68を制御して、表示部67に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池51の残量等の情報を表示させる。

【0073】さらに、ポータブルデバイス6は、EEPROM68に、フラッシュメモリ80に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ61のブロック位置及びその他の種々のメモリ蓄積情報等のいわゆるFAT（File Allocation Table）を格納する。

【0074】因みに、本実施の形態においては、コンテンツは、64KByteを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がFATに格納される。

【0075】フラッシュメモリ61にFATが格納される場合、例えば、1曲目のコンテンツがCPU53の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

【0076】このように、FATは、フラッシュメモリ61へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

【0077】FATがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書換えの回数に達してしまい、フラッシュメモリ61の書換えができなくなってしまう。

【0078】そこで、ポータブルデバイス6は、FATをEEPROM68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書換えの頻度を少なくしている。

【0079】書換えの回数の多いFATをEEPROM68に記憶させることにより、FATをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU53は、EEPROM68にFATを追記するように書き込ませるので、EEPROM68の同一の領域の書換えの頻度を少なくして、EEPROM68が短期間で書換え不能になることを防止する。

【0080】ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

【0081】ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

【0082】CPU53は、USB接続されたとき、DSP59のコンテンツの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【0083】このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

【0084】なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

【0085】つぎに、パーソナルコンピュータ1にイン

ストールされたプログラムの実行等により実現されるパーソナルコンピュータ1の機能について説明する。

【0086】図4は、所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を示す図である。

【0087】コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、コピー管理プログラム133、移動管理プログラム134、暗号方式変換プログラム135、圧縮方式変換プログラム136、暗号化プログラム137、利用条件変換プログラム139、利用条件管理プログラム140、認証プログラム141、復号プログラム142、PD用ドライバ143、購入用プログラム144及び購入用プログラム145などの複数のプログラムで構成されている。

【0088】コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0089】EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、EMDの登録の際に、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4（4-1、4-2、4-3）のとの接続を選択して、購入用アプリケーション115、又は購入用プログラム144、145に、EMDサーバ4（4-1、4-2、4-3）との通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0090】チェックイン／チェックアウト管理プログラム132は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに基づいて、コンテンツファイル161-1～161-Nに格納されているコンテンツをポータブルデバイス6にチェックアウトするか、又はポータブルデバイス6に記憶されているコンテンツをチェックインする。

【0091】チェックイン／チェックアウト管理プログラム132は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに格納されている利用条件情報を更新する。

【0092】コピー管理プログラム133は、コンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに基づいて、コンテンツファイル161-1～161-Nに格納されているコンテ

ツをポータブルデバイス6にコピーするか、又はポータブルデバイス6からコンテンツをコンテンツデータベース114にコピーする。

【0093】移動管理プログラム134は、コンテンツデータベース114に記録されている利用条件ファイル162-1～162-Nに基づいて、コンテンツファイル161-1～161-Nに格納されているコンテンツをポータブルデバイス6に移動するか、又はポータブルデバイス6からコンテンツをコンテンツデータベース114に移動する。

【0094】暗号方式変換プログラム135は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの暗号化の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの暗号化の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1～161-Nに格納されているコンテンツと同一の暗号化の方式に変換する。

【0095】圧縮方式変換プログラム136は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの圧縮の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの圧縮の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1～161-Nに格納されているコンテンツと同一の圧縮の方式に変換する。

【0096】暗号化プログラム137は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1～161-Nに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【0097】圧縮／伸張プログラム138は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1～161-Nに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム138は、符号化されているコンテンツを伸張（復号）する。

【0098】利用条件変換プログラム139は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの利用条件情報（いわゆる、Usage Rule）、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの利用条件情報を、コンテンツデータベース114が記録している利用条件ファイル162-1～162-Nに格納されている利用条件情報と同一のフォーマットに変換する。

【0099】利用条件管理プログラム140は、コンテ

ンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテンツデータベース114に記録されている利用条件ファイル162-1~162-Nに格納されている利用条件情報に対応するハッシュ値を基に、利用条件情報の改竄を検出する。利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース114に記録されている利用条件ファイル162-1~162-Nに格納されている利用条件情報を更新に対応して、利用条件情報に対応するハッシュ値を更新する。

【0100】認証プログラム141は、コンテンツ管理プログラム111と購入用アプリケーションプログラム115との相互認証の処理及びコンテンツ管理プログラム111と購入用プログラム144との相互認証の処理を実行する。また、認証プログラム141は、EMDサーバ4-3と購入用プログラム145との相互認証の処理で利用される認証鍵を記憶している。

【0101】認証プログラム141が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされたとき、認証プログラム141に記憶されておらず、表示操作指示プログラム112により登録の処理が正常に実行されたとき、EMD登録サーバ3から供給され、認証プログラム141に記憶される。

【0102】復号プログラム142は、コンテンツデータベース114が記録しているコンテンツファイル161-1~161-Nに格納されているコンテンツをパーソナルコンピュータ1が再生するとき、コンテンツを復号する。

【0103】PD用ドライバ143は、ポータブルデバイス6に所定のコンテンツをチェックアウトするとき、又はポータブルデバイスから所定のコンテンツをチェックインするとき、ポータブルデバイス6にコンテンツ又はポータブルデバイス6に所定の処理を実行させるコマンドを供給する。

【0104】購入用プログラム144は、コンテンツ管理プログラム111とともにインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCDに記録されて供給される。購入用プログラム144は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

【0105】購入用プログラム144は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム144を読み出しても、インストラクションを特定できないな

ど）ように構成されている。

【0106】購入用プログラム144は、ネットワーク2を介して、EMDサーバ4-2に所定のコンテンツの送信を要求するとともに、EMDサーバ4-2からコンテンツを受信する。また、購入用プログラム144は、EMDサーバ4-2からコンテンツを受信するとき、課金の処理を実行する。

【0107】購入用プログラム145は、コンテンツ管理プログラム111とともにインストールされるプログラムであり、ネットワーク2を介して、EMDサーバ4-3に所定のコンテンツの送信を要求するとともに、EMDサーバ4-3からコンテンツを受信する。また、購入用プログラム145は、EMDサーバ4-3からコンテンツを受信するとき、課金の処理を実行する。

【0108】表示操作指示プログラム112は、フィルタリングデータファイル181、表示データファイル182、画像ファイル183-1~183-K、又は履歴データファイル184を基に、ディスプレイ20に所定のウィンドウの画像を表示させ、キーボード18又はマウス19への操作を基に、コンテンツ管理プログラム111にチェックイン又はチェックアウトなどの処理の実行を指示する。

【0109】フィルタリングデータファイル181は、コンテンツデータベース114に記録されているコンテンツファイル161-1~161-Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD21に記録されている。

【0110】表示データファイル182は、コンテンツデータベース114に記録されているコンテンツファイル161-1~161-Nに格納されているコンテンツに対応するデータを格納して、HDD21に記録されている。

【0111】画像ファイル183-1~183-Kは、コンテンツデータベース114に記録されているコンテンツファイル161-1~161-Nに対応する画像、又は後述するパッケージに対応する画像を格納して、HDD21に記録されている。

【0112】以下、画像ファイル183-1~183-Kを個々に区別する必要がないとき、単に、画像ファイル183と称する。

【0113】履歴データファイル184は、コンテンツデータベース114に記録されているコンテンツファイル161-1~161-Nに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD21に記録されている。

【0114】表示操作指示プログラム112は、登録の処理のとき、ネットワーク2を介して、EMD登録サーバ3に、予め記憶しているコンテンツ管理プログラム111のIDを送信するとともに、EMD登録サーバ3か

ら認証用鍵及びEMD選択プログラム131を受信して、コンテンツ管理プログラム111に認証用鍵及びEMD選択プログラム131を供給する。

【0115】録音プログラム113は、所定のウィンドウの画像を表示させて、キーボード18又はマウス19への操作を基に、ドライブ22に装着された光ディスク42であるCDからコンテンツの録音時間などのデータを読み出す。

【0116】録音プログラム113は、CDに記録されているコンテンツの録音時間などを基に、ネットワーク2を介して、WWWサーバ5-1又は5-2にCDに対応するデータ（例えば、アルバム名、又はアーティスト名など）又はCDに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ5-1又は5-2からCDに対応するデータ又はCDに記録されているコンテンツに対応するデータを受信する。

【0117】録音プログラム113は、受信したCDに対応するデータ又はCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム112に供給する。

【0118】また、録音の指示が入力されたとき、録音プログラム113は、ドライブ22に装着された光ディスク42であるCDからコンテンツを読み出して、コンテンツ管理プログラム111に出力する。

【0119】コンテンツデータベース114は、コンテンツ管理プログラム111から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル161-1～161-Nのいずれかに格納する（HDD21に記録する）。コンテンツデータベース114は、コンテンツファイル161-1～161-Nにそれぞれ格納されているコンテンツに対応する利用条件情報を、コンテンツが格納されているコンテンツファイル161-1～161-Nにそれぞれ対応する利用条件ファイル162-1～162-Nのいずれかに格納する（HDD21に記録する）。

【0120】コンテンツデータベース114は、コンテンツファイル161-1～161-N又は利用条件ファイル162-1～162-Nをレコードとして記録してもよい。

【0121】例えば、コンテンツファイル161-1に格納されているコンテンツに対応する利用条件情報は、利用条件ファイル162-1に格納されている。コンテンツファイル161-Nに格納されているコンテンツに対応する利用条件情報は、利用条件ファイル162-Nに格納されている。

【0122】以下、コンテンツファイル161-1～161-Nを個々に区別する必要があるとき、単に、コンテンツファイル161と称する。以下、利用条件ファイル162-1～162-Nを個々に区別する必要がある

とき、単に、利用条件ファイル162と称する。

【0123】購入用アプリケーションプログラム115は、EMD登録サーバ3からネットワーク2を介して供給され、又は所定のCD-ROMに記録されて供給される。購入用アプリケーションプログラム115は、ネットワーク2を介して、EMDサーバ4-1に所定のコンテンツの送信を要求するとともに、EMDサーバ4-1からコンテンツを受信して、コンテンツ管理プログラム111に供給する。また、購入用アプリケーションプログラム115は、EMDサーバ4-1からコンテンツを受信するとき、課金の処理を実行する。

【0124】次に、表示データファイル182に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル161-1～161-Nとの対応付けについて説明する。

【0125】コンテンツファイル161-1～161-Nのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

【0126】オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

【0127】マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【0128】フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ4又はWWWサーバ5などからネットワーク2を介して供給され、又は所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

【0129】フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ1は、今週の日本の

ポップス1位のコンテンツ～今週の日本のポップス10位のコンテンツを特定することができる。

【0130】フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に“愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

【0131】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ221（コンテンツ用表示データ221に使用者が設定したデータを含む）、又は履歴データ184などと、フィルタリングデータとを対応させて選択される。

【0132】ドライバ117は、コンテンツ管理プログラム111などの制御の基に、音声入出力インターフェース24を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム111に供給するか、若しくはコンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツに対応するアナログ信号を出力する。

【0133】図5は、表示操作指示プログラム112を起動させたとき、操作指示プログラム112がディスプレイ20に表示させる表示操作指示ウィンドウの例を示す図である。

【0134】表示操作指示ウィンドウには、録音プログラム113を起動させるためのボタン201、EMD選択プログラム131を起動させるためのボタン202、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン203、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン204等が配置されている。

【0135】ボタン205が選択されているとき、フィールド211には、オリジナルパッケージに対応するデータが表示される。ボタン206が選択されているとき、フィールド211には、マイセレクトパッケージに対応するデータが表示される。ボタン207が選択されているとき、フィールド211には、フィルタリングパッケージに対応するデータが表示される。

【0136】フィールド211に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

【0137】例えば、図5においては、パッケージ名称“ファースト”及びアーティスト名“A太郎”、パッケージ名称“セカンド”及びアーティスト名“A太郎”などがフィールド211に表示される。

【0138】フィールド212には、フィールド211

で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド212に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

【0139】例えば、図5においては、パッケージ名称“セカンド”に対応するパッケージが選択されているので、パッケージ名称“セカンド”に対応するパッケージに属するコンテンツに対応する曲名“南の酒場”及びチェックアウト可能回数（例えば、8分音符の1つがチェックアウト1回に相当し、8分音符が2つでチェックアウト2回を示す）、並びに曲名“北の墓場”及びチェックアウト可能回数（8分音符が1つでチェックアウト1回を示す）などがフィールド212に表示される。

【0140】このように、フィールド212に表示されるチェックアウト可能回数としての1つの8分音符は、対応するコンテンツが1回チェックアウトできることを示す。

【0141】フィールド212に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が0である。（ただし、パーソナルコンピュータ1はそのコンテンツを再生することができる。））ことを示す。また、フィールド212に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

【0142】なお、チェックアウト可能回数は、図5に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【0143】また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図4の画像ファイル183-1～183-Kのいずれかに対応する）を表示させるフィールド208が配置されている。ボタン209は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ45に出力させる）とき、クリックされる。

【0144】ボタン205が選択され、フィールド211に、オリジナルパッケージに対応するデータが表示されている場合、フィールド212に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、選択されている曲名に対応する、コンテンツデータベース114に格納されている所定のコンテンツを消去させる。

【0145】録音プログラム113が表示させるウィンドウのボタン（後述するボタン255）が選択されて（アクティブにされて）いる場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、表示操作指

示ウィンドウに、予め指定されているポータブルデバイス6に記憶されているコンテンツの曲名を表示するフィールド213を表示する。

【0146】録音プログラム113が表示させるウィンドウのボタンが選択されている場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、コンテンツデータベース114に記録した、CDから読み出したコンテンツを予め指定されているポータブルデバイス6にチェックアウトさせる。

【0147】フィールド213にはコンテンツの曲名に対応させて、フィールド213の最も左に、そのコンテンツがパーソナルコンピュータ1にチェックインできるか否かを示す記号が表示される。例えば、フィールド213の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできる（すなわち、パーソナルコンピュータ1からチェックアウトされた）ことを示している。フィールド213の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできない（すなわち、パーソナルコンピュータ1からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【0148】表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6に記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス6に記憶されているコンテンツが属するパッケージ）の名称を表示するフィールド214、フィールド213を閉じるためのボタン210及びチェックイン又はチェックアウトを実行させるボタン215を表示する。

【0149】更に、表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、フィールド212で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン216、フィールド213で選択された曲名に対応するコンテンツのチェックインを設定するボタン217、フィールド213に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン218及びチェックイン又はチェックアウトの設定を取り消すボタン219を配置させる。

【0150】ボタン216乃至219の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ1は、チェックイン又はチェックアウトの処理を実行しない。

【0151】ボタン216乃至219の操作によるチェックイン又はチェックアウトの設定をした後、ボタン215がクリックされたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン215がクリックされたとき、表示操作指示プログラム112は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム111に、ポータブルデバイス6にコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス6が記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル162に格納されている利用条件情報を更新させる。

【0152】チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム112は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル184に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス6の名称などから成る。

【0153】チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

【0154】図6は、録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。

【0155】例えば、WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド251に、“アシンクロナイズド”などのCDのタイトルを表示する。WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド252に、例えば、“クワイ”などのアーティスト名を表示する。

【0156】WWWサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド253の曲名を表示する部分に、例えば、“ヒート”、“プラネット”、“ブラック”、“ソウル”などの曲名を表示する。同様に、録音プログラム113は、フィールド253のアーティストを表示する部分に、例えば、“クワイ”などのアーティスト名を表示する。

【0157】録音プログラム113が所定のCDの情報を受信した後、録音プログラム113は、HDD21の所定のディレクトリにCDの情報を格納する。

【0158】ボタン254などがクリックされて、CDの情報の取得の指示を受けたとき、録音プログラム113は、始めに、HDD21の所定のディレクトリを検索する。録音プログラム113は、そのディレクトリにCDの情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されているCDの情報を利用するか否かを選択させる。

【0159】録音プログラム113が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン256がクリックされたとき、録音プログラム113は、ドライブ22に格納されているCDからコンテンツを読み出して、CDから読み出したコンテンツをCDの情報とともにコンテンツ管理プログラム111に供給する。コンテンツ管理プログラム111の圧縮／伸張プログラム138は、録音プログラム113から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム137は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム139は、圧縮され、暗号化されたコンテンツに対応する利用条件情報を生成する。

【0160】コンテンツ管理プログラム111は、圧縮され、暗号化されたコンテンツを利用条件情報とともに、コンテンツデータベース114に供給する。

【0161】コンテンツデータベース114は、コンテンツ管理プログラム111から受信したコンテンツに対応するコンテンツファイル161及び利用条件ファイル162を生成して、コンテンツファイル161にコンテンツを格納するとともに、利用条件ファイル162に利用条件情報を格納する。

【0162】コンテンツ管理プログラム111は、コンテンツデータベース114にコンテンツ及びコンテンツに対応する利用条件情報が格納されたとき、録音プログラム113から受信したCDの情報及び利用条件情報を表示操作指示プログラム112に供給する。

【0163】表示操作指示プログラム112は、録音の処理でコンテンツデータベース114に格納されたコンテンツに対応する利用条件情報及びCDの情報を基に、表示データファイル182に格納する表示用のデータを生成する。

【0164】録音プログラム113が表示させるウィンドウには、更に、CDから読み出したコンテンツをコンテンツデータベース114に記録したとき、自動的に、CDから読み出したコンテンツをポータブルデバイス6にチェックアウトさせるか否かの設定を行うボタン255が配置されている。

【0165】例えば、ボタン255がクリックされたとき、録音プログラム113は、ポータブルデバイス6を示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス6の選択をしたとき、選択されたポータブルデバイス6に自動的に、

CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから“チェックアウトしない”を選択した場合、パーソナルコンピュータ1は、CDからコンテンツを記録したとき、チェックアウトしない。

【0166】このように、録音プログラム113が表示させるウィンドウのボタン255をアクティブにしておくだけで、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、パーソナルコンピュータ1は、予め指定されているポータブルデバイス6に、CDから読み出したコンテンツをチェックアウトさせることができる。

【0167】(2) 異なるフォーマット間での取り扱いところで、音楽コンテンツを提供するコンテンツ配信業者は、数多く存在し、それぞれの配信業者毎に、そのコンテンツの暗号化方式や圧縮方式、さらに、利用条件情報のフォーマットが異なっている。従って、一般にユーザは、提供を受けたいコンテンツの配信業者毎に、再生やチェックイン／チェックアウト用のコンテンツ管理アプリケーションやポータブルデバイスを購入しなければならなかった。そのため、ユーザは、1つのパーソナルコンピュータ上に格納されている音楽コンテンツを、1つの管理アプリケーションやポータブルデバイスで取り扱うことができなかった。

【0168】そこで、本システムでは、このように配信業者毎にフォーマットが異なるコンテンツを、パーソナルコンピュータ1上で統一的に取り扱っている。

【0169】以下、この音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて、図7を参照して説明する。

【0170】ネットワーク2に接続された複数のEMDサーバは、例えば音楽提供会社Aから提供される音楽コンテンツを配信するEMDサーバ(A)4-1、音楽提供会社Bから提供される音楽コンテンツを配信するEMDサーバ(B)4-2、音楽提供会社Xから提供される音楽コンテンツを配信するEMDサーバ(X)4-3であるものとする。各EMDサーバ4(4-1, 4-2, 4-3)は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパーソナルコンピュータ1にネットワーク2を介して提供を行う。また、各EMDサーバ4(4-1, 4-2, 4-3)では、音楽コンテンツの暗号化方式、利用条件(Usage Rule)情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等が各社独自の方式が採用されそれぞれ異なる方式により音楽コンテンツを配信している。

【0171】パーソナルコンピュータ1には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、EMDサーバ(A)4-1から音楽コンテンツの購入や管理や再生を行う再生用アプリケー

ション(A)311と、EMDサーバ(B)4-2から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション(B)312と、音楽コンテンツをポータブルデバイス(A)6-1に転送するデバイスドライバ(A)313と、音楽コンテンツをポータブルデバイス(B)6-2に転送するデバイスドライバ(B)314とがインストールされている。なお、この図7で示す再生用アプリケーション311、312は、図4で示した購入用アプリケーションプログラム115及びドライバ117に対応するものである。

【0172】また、パーソナルコンピュータ1には、HDD21内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット(X)315がインストールされている。この包括管理ユニット(X)315は、さらに、EMD用受信インターフェース316、EMD用送信インターフェース317、PD用ドライバ318により構成されている。

【0173】また、ここでは、ポータブルデバイス(A)6-1は音楽提供会社Aに対応した専用の装置であり、ポータブルデバイス(B)6-2は音楽提供会社Bに対応した専用の装置であり、ポータブルデバイス(X)6-3は音楽提供会社Xに対応した専用の装置であるものとする。なお、ここでは、メモリカード内に格納した音楽コンテンツは、各音楽提供会社独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっているものとする。

【0174】再生用アプリケーション(A)311は、EMDサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション(A)311は、対応しているEMDサーバに対してのみ接続処理を行うようになっている。ここでは、再生用アプリケーション(A)311は、EMDサーバ(A)4-1に対応した処理を行い、他のEMDサーバに対して接続処理を行うことができない。また、再生用アプリケーション(A)311は、EMDサーバ(A)4-1と接続した際の認証処理、ポータブルデバイス(A)6-1と接続した際の認証処理、HDD21に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション(A)311は、例えば、EMDサーバ(A)4-1からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、HDD21に格納する。なお、暗号化処理の方式は、各再生用アプリケーションでそれぞれ独自の方式を採用している。そのため、パーソナルコンピュータ1内の同一のHDD21に格納されている音楽コンテンツであっても、専用の再生用ア

プリケーションでなければ、他の再生用アプリケーションでは暗号を解読することができないようになっている。

【0175】また、再生用アプリケーション(A)311は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション(A)311は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を1回分デクリメントする等の処理を行う。

【0176】また、再生用アプリケーション(A)311は、自己がHDD21上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット(X)315のEMD用受信インターフェース316に送信する。

【0177】再生用アプリケーション(B)312は、EMDサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ、コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション(B)312は、対応しているEMDサーバに対してのみ接続処理を行うようになっている。具体的には、再生用アプリケーション(B)312は、EMDサーバ(B)4-2に対応した処理を行い、他のEMDサーバに対して接続処理を行うことができない。また、再生用アプリケーション(B)312は、EMDサーバ(B)4-2と接続した際の認証処理、ポータブルデバイス(B)6-2と接続した際の認証処理、HDD21に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション(B)312は、例えば、EMDサーバ(B)4-2からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、HDD21に格納する。

【0178】また、再生用アプリケーション(B)312は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション(B)312は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を1回分デクリメントする等の処理を行う。

【0179】また、再生用アプリケーション(B)312は、自己がHDD21上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット(X)315のEMD用受信インターフェース316に送信する。

【0180】デバイスドライバ(A)313は、ポータブルデバイス(A)6-1への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ(A)313は、ポータブルデバイス(A)6-1に音楽コンテンツを転送する。

【0181】デバイスドライバ(B)314は、ポータ

ブルデバイス(B)6-2への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ(B)314は、ポータブルデバイス(B)6-2に音楽コンテンツを転送する。

【0182】包括管理ユニット(X)315は、EMDサーバ(X)4-3から音楽コンテンツの提供を受ける音楽提供会社X専用のアプリケーションソフトウェアであるとともに、デバイスドライバ(A)313及びデバイスドライバ(B)314や、再生用アプリケーション(A)311及び再生用アプリケーション(B)312との間で音楽コンテンツ及び利用条件情報の転送を行って、パーソナルコンピュータ1内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス(X)6-3に転送することができる。

【0183】なお、この包括管理ユニット(X)115は、図4に示したコンテンツ管理プログラム111に対応する処理を行う。

【0184】PD用ドライバ318は、ポータブルデバイス(X)6-3との接続用のインターフェースモジュールで、このポータブルデバイス(X)6-3との間における認証処理や暗号化処理を行う。また、PD用ドライバ318は、他のポータブルデバイス8、9に音楽コンテンツ等を転送する場合には、デバイスドライバ(A)313やデバイスドライバ(B)314を介して音楽コンテンツ及び利用条件情報を転送する。

【0185】EMD用受信インターフェース316は、再生用アプリケーション(A)311及び再生用アプリケーション(B)312からの音楽コンテンツ及び利用条件情報の受信、EMDサーバ(X)4-3からネットワーク2を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、PD用ドライバ318との間での音楽コンテンツ及び利用条件情報の送受信を行う。

【0186】EMD用受信インターフェース316は、再生用アプリケーション(A)311及び再生用アプリケーション(B)312から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、再生用アプリケーション(A)311及び再生用アプリケーション(B)312が用いている方式から、包括管理ユニット(X)315が用いている方式に変換される。ここで包括管理ユニット(X)315が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、EMD用受信インターフェース316は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、PD用ドライバ318を介してデバイスドライバ(A)313やデバイスドライバ

(B)314に送信する。また、EMD用受信インターフェース316は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、PD用ドライバ318を介して、ポータブルデバイス(X)6-3に送信する。

【0187】このように、EMDサーバ(A)4-1及びEMDサーバ(B)4-2から提供される音楽コンテンツは、一旦再生用アプリケーション(A)311及び再生用アプリケーション(B)312によりダウンロードされ、音楽コンテンツの暗号化方式、圧縮方式、利用条件情報が、統一転送プロトコルに変換されて、包括管理ユニット(X)315に転送される。包括管理ユニット(X)315は、EMDサーバ(A)4-1、EMDサーバ(B)4-2、EMDサーバ(X)4-3からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行うことができる。

【0188】また、EMD用受信インターフェース316は、音楽コンテンツの複製(コピー)、移動(ムーブ)、チェックイン、チェックアウトの機能を有している。

【0189】EMD用受信インターフェース316は、ユーザからの複製命令、移動命令に従い、例えば、再生用アプリケーション(A)311や再生用アプリケーション(B)312によって管理されている音楽コンテンツを、包括管理ユニット(X)315に複製や移動する処理を行う。この際に、EMD用受信インターフェース316は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

【0190】また、ユーザからのCDリッピング命令やチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス6(6-1、6-2、6-3)に格納されている音楽コンテンツを、包括管理ユニット(X)315に複製やチェックインする処理を行う。この際に、EMD用受信インターフェース316は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【0191】また、ユーザからのチェックアウト命令に従い、包括管理ユニット(X)315により管理されている音楽コンテンツを、ポータブルデバイス(X)6-3に記録する処理を行う。この際に、EMD用受信インターフェース316は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。また、この際に、利用条件のチェックアウト可能回数を1減少させる。

【0192】また、包括管理ユニット(X)315では、図8に示すように、アプリケーション層の下位レイ

ヤに統一転送プロトコルを設けて、このレイヤにおいて他の再生用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット(X)315は、この統一転送プロトコルの更に下位レイヤをhttp(hyper Text Transfer Protocol)として、EMDサーバ(X)4-3とのデータ送受信を行っている。

【0193】以上のような構成の音楽コンテンツ配信システムでは、EMDサーバ(A)4-1及びEMDサーバ(B)4-2から配信された音楽コンテンツを、包括管理ユニット(X)315が取得し、再生や管理を行うようになっている。そして、EMDサーバ(X)4-3、EMDサーバ(A)4-1及びEMDサーバ(B)4-2から配信された音楽コンテンツを、ポータブルデバイス(X)6-3へ転送できるようになっている。

【0194】このように音楽コンテンツ配信システムでは、包括管理ユニット(X)315を中心として、各再生用アプリケーション及びデバイスドライバの間で、転送する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの転送が行われる。そのため、例えば、再生用アプリケーション(A)311によりEMDサーバ(A)4-1からダウンロードした音楽コンテンツ並びに再生用アプリケーション(B)312によりEMDサーバB4-2からダウンロードした音楽コンテンツを、包括管理ユニット(X)315に転送することができる。このため、例えば音楽提供会社Aからのみ提供されるアーティストの音楽コンテンツを、ポータブルデバイス(X)6-3に転送することができる。すなわち、この音楽コンテンツ配信システムでは、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パーソナルコンピュータ1のハードディスク内に格納されている様々な方式の音楽コンテンツを、包括管理ユニット(X)315やポータブルデバイス(X)6-3により再生を行うことができる。特に、音楽コンテンツ配信システムでは、転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

【0195】すなわち、音楽コンテンツ配信システムでは、音楽コンテンツの再生や制御を行う再生用アプリケーション間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システムでは、複数の再生用アプリケーションが存在してもパーソナルコンピュータ1内の例えばHDD21に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。ま

た、音楽コンテンツとともに利用条件情報も転送するので、1つの音楽コンテンツに対して利用条件が重複したりすることがなく、音楽コンテンツの著作権も確実に保護することができる。

【0196】(3)利用条件情報

(一般的に用いられる利用条件情報の説明)つぎに、再生用アプリケーション(A)311に用いられる利用条件情報のフォーマットの一例について説明をする。

【0197】再生用アプリケーション(A)311では、例えば、図9(a)に示すような表形式で記述された利用条件情報が用いられている。

【0198】表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日(from)、再生終了日(to)、1回の再生に対する価格(pay/play)等が記述される。このような利用条件情報は、図9(b)に示すように各音楽コンテンツに付加された状態で、EMDサーバ(A)4-1から配信される。再生用アプリケーション(A)311は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日(from)が99年10月25日、再生終了日(to)が99年11月24日、1回の再生に対する価格(pay/play)がyes/10円と記述されているとする。この場合、その音楽コンテンツは、99年10月25日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、99年11月24日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、1回の再生の度に10円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として保管しておき、そのログ情報をEMDサーバ(A)4-1にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

【0199】(包括管理ユニット(X)315が用いている利用条件情報の説明)つぎに、包括管理ユニット(X)315が用いている利用条件情報について説明する。

以下説明をする利用条件情報は、EMDサーバ(X)4-3からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット(X)315がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、再生用アプリケーション

(A)311と包括管理ユニット(X)315との間、及び、再生用アプリケーション(B)312と包括管理ユニット(X)315との間で、音楽コンテンツの転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

【0200】統一利用条件情報は、図10に示すように、インデックスファイル331、オートマトンファイ

ル332と、パラメータファイル333と、履歴ファイル334とから構成される。各ファイルは、XML(extendible Markup Language)言語で記述されている。

【0201】インデックスファイル331には、各ファイルのリファレンス情報等が記述されている。

【0202】オートマトンファイル332には、図11に示すように、利用条件がオートマトンで記述されたオートマトン記述部341と、コンテンツ鍵による認証コード(MAC:Message Authentication Code)342、コンテンツ提供者の署名(Sig)343、この署名を検証するための認証書(Cert)344が付加されている。ここで、コンテンツ鍵を K_C 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K^{-1}_E 、 K^1_E とする。

【0203】オートマトン記述部341は、tuple列で記述されたExtended State Machineにより音楽コンテンツの動作状態が記述される。

【0204】具体的には、オートマトン記述部341では、現在の音楽コンテンツの動作状態の集合を Q とし、音楽コンテンツのイベントを表す入力シンボルの集合を Σ とし、状態遷移した後の音楽コンテンツの動作状態の集合を Q' を以下のように表す。

$$Q' = \{d \mid d = \delta(q, \alpha) \mid q \in Q, \alpha \in \Sigma, \delta: Q \times \Sigma \rightarrow Q\}$$

この式に示すように、状態遷移した後の状態 Q' の集合は、 d として表される。この d は、変数 q 、 α をもった関数 δ によって定義される。 q は、音楽コンテンツの動作状態の集合 Q のなかの1つの動作状態を示している。 α は、イベントの集合 Σ のなかの1つのイベントを示している。そして、関数 δ は、 Q 及び Σ のべき集合の Q への写像である。

【0205】そして、以上の Q 、 Σ 、 Q' に基づき、各tupleを

$$\{ \langle q, \alpha, d \rangle \mid q, d \in Q, \alpha \in \Sigma \}$$

として表す。なお、 $\langle q, \alpha, d \rangle$ は、 q 、 α 、 d の順列のある組み合わせを示している。

【0206】ここで、 Σ には、再生(Play)、複製(copy)、支払い金額(pay Y)、再生開始可能日時(from YMD)、再生終了日時(to YMD)、使用可能日数(in Ddays)、ヌルイベント(ϵ)といったイベントが、以下のように記述される。

$$\Sigma = \{\text{Play}, \text{copy}, \text{pay Y}, \text{from YMD}, \text{to YMD}, \text{in Ddays}, \epsilon\}$$

このようにオートマトン記述部341は、以上のように記述される。

【0207】このオートマトン記述部341への具体的な記述例について説明をする。

【0208】例えば、図12に示すような音楽コンテンツの動作遷移を示すオートマトンのtuple列による記述例を、図13に示す。

【0209】このオートマトンは、以下に説明するような状態遷移をする。

【0210】まず、初期状態 q_0 から、状態 q_1 及び状態 q_5 に遷移する。状態 q_1 及び状態 q_5 以降は、それぞれ並行して動作する。

【0211】状態 q_1 で、所定金額(例えば10円)の支払いイベント(pay 10)が発生すると状態 q_2 へ遷移する。状態 q_2 で、プレイイベント(play)が発生すると状態 q_1 へ遷移する。すなわち、このオートマトンでは、10円の支払いがされると、音楽コンテンツが1回だけ再生が可能となることを示している。また、状態 q_1 で、所定金額(例えば1000円)の支払いイベント(a. pay 1000)が発生すると状態 q_3 へ遷移する。状態 q_3 では、プレイイベント(play)が発生すると、再度この状態 q_3 に遷移する。すなわち、このオートマトンでは、1000円の支払いがされると、音楽コンテンツが回数に制限無く再生が可能となることを示している。また、状態 q_1 で、一回の再生金額(例えば10円)の n 倍の金額の支払いイベント(pay 10 \times n)が発生すると、状態 q_4 へ遷移する。状態 q_4 へ遷移してから、プレイイベント(play)が発生すると、再度この状態 q_4 に遷移する。そして、この状態 q_4 で、 n 回のプレイイベントが発生すると、状態 q_1 に遷移する。すなわち、このオートマトンでは、10 \times n円の支払いがされると、音楽コンテンツが n 回再生が可能となることを示している。

【0212】また、状態 q_5 で、所定金額(例えば100円)の支払いイベント(pay 100)が発生すると状態 q_6 へ遷移する。状態 q_6 で、コピーイベント(copy)が発生すると状態 q_5 へ遷移する。また、状態 q_6 で、コピーイベント(copy)が発生すると、状態 q_8 へ遷移する。状態 q_8 で、プレイイベント(play)が発生すると、再度この状態 q_8 に遷移する。また、この状態 q_8 で、コピーイベント(copy)が発生すると、状態 q_9 に遷移する。状態 q_9 では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、100円の支払いがされると音楽コンテンツを他のデバイスへ1回コピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【0213】また、状態 q_5 で、所定金額(例えば2000円)の支払いイベント(a. pay 2000)が発生すると状態 q_7 へ遷移する。状態 q_7 では、コピーイベント(copy)が発生すると、再度この状態 q_7 に遷移する。また、状態 q_7 で、コピーイベント(copy)が発生すると、状態 q_8 へ遷移する。状態 q_8 で、プレイイベント(play)が発生すると、再度この状態 q_8 に遷移する。また、この状態 q_8 で、コピーイベ

ント (copy) が発生すると、状態 q_9 に遷移する。状態 q_9 では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、2000円の支払いがされると、音楽コンテンツを他のデバイスへ回数制限無くコピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【0214】そして、以上のように状態遷移をするオートマトンをtuple列で記述すると、図13に示すようになる。

【0215】また、オートマトン記述部341は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作 a_0 と動作 a_1 との並列

$\langle q_0, \text{pay}100, q_1, a. n := a. n - 100 \rangle \dots (1)$

$\langle q_0, \text{pay}(a. n), q_1, a. n := 0 \rangle \dots (2)$

$\langle q_1, \text{play}, q_2 \rangle \dots (3)$

この例は、1つの音楽コンテンツの買い取り値段 {式(1)} が、アルバム買い取り {式(2)} の値段に影響を及ぼすことを示している。

【0216】以上のようなオートマトン記述部341は、図14に示すように、エントリーID345と、コンテンツID346と、バージョン情報347と、変数情報348と、tuple列349とから構成される。

【0217】以上のように記述フォーマットが定められたオートマトン記述部341の具体例について説明をする。

【0218】なお、以下にオートマトンの記述で用いられているイベント及びコマンドは、XMLの仕様に基いて規定されたDTD (Document Type Definition) で定義されている。例えば、図15に示すように、再生動作 (play)、複製動作 (copy)、再生権購入 (pay-for-play)、複製権購入 (pay-for-copy)、アルバム再生権購入 (pay-for-album-play)、アルバム複製権購入 (pay-for-album-copy)、使用可能開始日 (from)、使用終了日 (to)、ヌル動作 (null) がイベントとして、DTDによって定義されている。

【0219】図16は、音楽コンテンツが1999年9月1日から再生が可能であることを示すXML言語によるオートマトン記述部341の記述例である。

【0220】この図16に示す記述は、図17に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q_1 と、状態 q_2 とから構成される。状態 q_1 で、日付が使用可能開始日 (from) の1999年9月1日となると、状態 q_2 へ遷移する。そして、状態 q_2 で、再生イベント (play) が発生すると、音楽コンテンツの再生を行い、再度状態 q_2 へ遷移する。このようにこのオートマトンは、音楽コンテンツを、1999年9月1日から再生を可能とするように制御してい

合成は、tuple列で以下のように表される。

$\langle q_0, a, a_0, q_0 \rangle$

$\langle q_0, a, a_1, q_0 \rangle$

また、オートマトン記述部341には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tupleで以下のように表される。

$\langle q_0, a, q_1; \text{action} \rangle$

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、IDとスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム (a) の買い取りの値段を表す変数を n とし、 $a. n := 1000$ のように記述する。このように変数に対するアクションが記述されたオートマトン記述部341の一例を以下に示す。

る。

【0221】図18は、音楽コンテンツが1999年10月31日まで再生が可能であることを示すXML言語によるオートマトン記述部341の記述例である。

【0222】この図18に示す記述は、図19に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q_1 と、終端状態の状態 end とから構成される。状態2で、再生イベント (play) が発生すると、音楽コンテンツの再生を行い、再度状態 q_2 へ遷移する。また、状態2で、使用終了日 (to) の1999年10月31日となると、状態 end へ遷移する。状態 end となると、どの状態へも遷移せずイベントも発生しない。このように、このオートマトンは、音楽コンテンツを、1999年10月31日まで再生を可能とするように制御している。

【0223】図20は、音楽コンテンツの再生可能期間が1999年9月1日から1999年10月31日までであって、且つ、その再生可能回数が16回であることを示すXML言語によるオートマトン記述部341の記述例である。

【0224】この図20に示す記述は、図21に示すようなオートマトンとなる。このオートマトンは、初期状態の状態 q_1 と、状態 q_2 と、終端状態の状態 end とから構成される。状態 q_1 で、使用可能開始日 (from) の1999年9月1日となると、状態 q_2 へ遷移する。そして、状態 q_2 で、再生イベント (play) が発生すると、音楽コンテンツの再生を行い、再度状態 q_2 へ遷移する。また、状態2で、使用終了日 (to) の1999年10月31日となるか、或いは、16回再生イベント (play \times 16) が発生すると、状態 end へ遷移する。状態 end となると、どの状態へも遷移せずイベントも発生しない。このようにこのオートマトン

は、音楽コンテンツの再生期間を1999年9月1日から1999年10月31日までとし、且つ、その再生回数を16回に制御している。

【0225】図22は、音楽コンテンツの再生回数を16回に制限することを示すXML言語によるオートマトン記述部341の記述例である。

【0226】つぎに、パラメータファイル333には、図23に示すように、パラメータ記述部351、コンテンツ鍵による認証コード352、コンテンツ提供者の署名353、この署名を検証するための認証書354が付加されている。ここで、コンテンツ鍵を K_c 、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ K^{-1}_E 、 K^1_E とする。

【0227】また、パラメータファイル333は、上記オートマトンファイル332を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル333は、図24に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティID55が付加される。ここで、 K'_c は、二次提供者のコンテンツ鍵で、 $K'_c = H(K_c, \text{EntityID})$ となる。なお、ここで、 H は、一方向ハッシュ関数である。二次提供者のコンテンツ鍵 K'_c は、一次提供者のコンテンツ鍵 K_c から作成される。一次提供者と二次提供者とは、その認証書により区別される。

【0228】パラメータファイル333を検証する方法としては、コンテンツ鍵が得られていればMACにより行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

【0229】MACにより検証するプロトコルは以下のようになる。コンテンツの一次提供者をS、二次提供者をA、端末をBとする。S→Aは、SからAへの伝送を示しており、S→Bは、SからBへの伝送を示しており、A→Bは、AからBへの伝送を示している。また、 ID_A は、デバイスAのIDを示している。

【0230】S→A: $K'_c = H(K_c, ID_A)$
S→B: $X = E_{K_S}(K_c)$
A→B: $ID_A, \text{Parameters}, M = \text{MAC}_{K'_c}(\text{Parameters})$

B: $M \text{ MAC}_{K'_c}(\text{Parameters})?$

このパラメータ記述部351には、上記オートマトンファイル31のオートマトン部41に記述された値の変更のための関数の係数が記述される。例えば、図13に示した例において、オートマトン部41では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

$\langle q_0, \text{pay}(f_1(10)), q_1 \rangle$

$\langle q_1, \text{pay}(f_2(10) \times n), q_2 \rangle$

この場合、上記関数 f_1 及び f_2 を、例えば、以下のよう

に定める。

$f_1(n) = 0.9n$

$f_2(n) = 90 + 0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル333を書き換えて、価格を変更することができる。

【0231】以上のようなパラメータ記述部351は、図25に示すように、エントリーID356と、コンテンツID357と、係数情報358とから構成される。

【0232】履歴ファイル334は、オートマトン記述部341に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。この履歴ファイル334には、上記オートマトン記述41のtuple内のステータスと変数を記録する。例えば、上述した図13に例において、2回再生を行った場合には、

$\langle q_0, q_1, q_0, q_1 \rangle$

となり、これにより以下のような動作の軌跡を得ることができる。

$\langle \text{pay}10, \text{play}, \text{pay}10, \text{play} \rangle$

これを集計して、例えば、包括管理ユニット(X)315にアップロード等すれば、ユーザの支払い金額を計算することができる。

【0233】以上のように音楽コンテンツ配信システムでは、ポリシー自体及びその具体的な値をプログラム化したオートマトンによって利用条件情報を記述しているので、コンテンツの利用条件の記載の自由度を高めることができる。

【0234】(4)破壊された音楽コンテンツ等のリストアップ及び再ダウンロード

つぎに、包括管理ユニット(X)315による音楽コンテンツのバックアップについて説明をする。

【0235】まず、包括管理ユニット(X)315の音楽コンテンツの鍵管理方法について、図26を用いて説明する。

【0236】包括管理ユニット(X)315は、パーソナルコンピュータ1内のHDD21に、音楽コンテンツC1, C2, C3...Cnを格納している。また、包括管理ユニット(X)315は、各音楽コンテンツC1, C2, C3...Cnに対応するコンテンツ鍵 K_{c1} , K_{c2} , K_{c3} ... K_{cn} も格納している。コンテンツ鍵 K_c は、音楽コンテンツCに対して一対一の関係となっている。また、各音楽コンテンツC1, C2, C3...Cnには、それぞれの識別するためのコンテンツIDが付加されている。このコンテンツIDを、CID1, CID2, CID3...CIDnとする。

【0237】音楽コンテンツC1, C2, C3...Cnは、コンテンツ鍵 K_{c1} , K_{c2} , K_{c3} ... K_{cn} により暗号化され、 $E(K_{c1}, C1)$, $E(K_{c2}, C2)$, $E(K_{c3}, C3)$... $E(K_{cn}, C$

n)とされた状態でパーソナルコンピュータ1のHDD 21内に記録されている。ここで、 $E(K, C)$ は、鍵KでコンテンツCを暗号化していることを示す。通常、コンテンツIDは、音楽コンテンツCのヘッダなどに記録されて音楽コンテンツCとともに暗号化されているか、或いは、MACが音楽コンテンツCに付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。

【0238】また、コンテンツ鍵 $Kc1, Kc2, Kc3 \dots Kcn$ は、ストレージ鍵KSにより暗号化され、 $E(KS, Kc1), E(KS, Kc2), E(KS, Kc3) \dots E(KS, Kcn)$ とされた状態でパーソナルコンピュータ1のHDD 21上に記録されている。このストレージ鍵KSは、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。

【0239】以上のように鍵管理が行われる包括管理ユニット(X)315では、例えば、音楽コンテンツC1の再生を行う場合には、ストレージ鍵KSを用いてコンテンツ鍵 $Kc1$ の暗号を解除し、続いて、このコンテンツ鍵 $Kc1$ を用いて、音楽コンテンツC1の暗号を解除する。このことにより、包括管理ユニット(X)315は、音楽コンテンツC1の再生を行うことができる。

【0240】また、以上のように鍵管理が行われる包括管理ユニット(X)315では、例えば、音楽コンテンツC1をHDD 21からポータブルデバイス(X)6-3に移動(MOVE)する場合には、ポータブルデバイス(X)6-3との間で相互認証を行い、認証が完了するとストレージ鍵KSを用いてコンテンツ鍵 $Kc1$ の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵 $Kc1$ を暗号化し、暗号化したコンテンツ鍵 $Kc1$ 及び暗号化した音楽コンテンツC1をポータブルデバイス

(X)6-3に転送する。そして、コンテンツ鍵 $Kc1$ と音楽コンテンツC1とともにHDD 21から消去をする。このことにより、包括管理ユニット(X)315は、音楽コンテンツC1をポータブルデバイス(X)6-3に移動することができる。

【0241】つぎに、HDD 21が破壊した場合など、音楽コンテンツやコンテンツ鍵をHDD 21から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

【0242】まず、通常時において、包括管理ユニット(X)315は、暗号化した音楽コンテンツC及びコンテンツ鍵 Kc のバックアップデータを、HDD 21内や他の記録媒体等に保存しておく。

【0243】また、通常時において、包括管理ユニット(X)315は、EMDサーバ(X)4-3からダウンロードした音楽コンテンツの購入記録と、HDD 21内に記憶している全ての音楽コンテンツのコンテンツIDのリストとを、使用ログ情報として管理する。このログ

情報は、音楽コンテンツをEMDサーバ(X)4-3からダウンロードしたときや、ポータブルデバイス(X)6-3への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。また、ログ情報は、HDD 21の別領域や他の記録媒体に格納しておく。包括管理ユニット(X)315は、このログ情報を、定期的、或いは、アクセスした度に、EMDサーバ(X)4-3にアップロードする。

【0244】そして、包括管理ユニット(X)315のHDD 21に格納されている音楽コンテンツCやコンテンツ鍵 Kc が破壊されてしまった場合には、以下に示すような処理が行われる。

【0245】音楽コンテンツCやコンテンツ鍵 Kc が破壊されてしまった場合、包括管理ユニット(X)315は、まず、EMDサーバ(X)4-3にアクセスを行って、ユーザ認証を行う。

【0246】続いて、EMDサーバ(X)4-3は、認証したユーザのユーザIDから、包括管理ユニット

(X)315の使用ログ情報を参照して、整合検証値ICV(Integrity Check Value)を生成する。この整合検証値ICVは、使用ログ情報に記述されている音楽コンテンツCのコンテンツIDであるCIDと、包括管理ユニット(X)315のストレージ鍵KSとに基づき、以下のように生成される。 $ICV = H(KS, CID1 || CID2 || \dots || CIDn)$ ここで、 $H(K, Data)$ は、一方向ハッシュ関数で、鍵Kによりその値が変化するものである。

【0247】続いて、EMDサーバ(X)4-3は、生成した整合検証値ICVを、包括管理ユニット(X)315に送信する。

【0248】続いて、包括管理ユニット(X)315は、音楽コンテンツC又はコンテンツ鍵 Kc がバックアップされていれば、そのバックアップデータをリストアップして、音楽コンテンツC又はコンテンツ鍵 Kc をHDD 21内に保存する。また、音楽コンテンツC又はコンテンツ鍵 Kc がバックアップされていなければ、EMDサーバ(X)4-3から破壊された音楽コンテンツC又はコンテンツ鍵 Kc を再配信してもらう。このとき、EMDサーバ(X)4-3は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

【0249】包括管理ユニット(X)315は、以上の処理を行い、破壊された音楽コンテンツC又はコンテンツ鍵 Kc を復活させる。

【0250】そして、包括管理ユニット(X)315は、復活された音楽コンテンツC又はコンテンツ鍵 Kc の再生や制御を行う場合には、上記整合検証値ICVによりその音楽コンテンツのCIDをチェックするようにする。このように、整合検証値ICVを用いて復活させた音楽コンテンツC又はコンテンツ鍵 Kc をチェックす

ることにより、例えば、ある音楽コンテンツ C_i をポータブルデバイス(X)6-3に移動してHDD21上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツ C_i である $E(K_{ci}, C_i)$ を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

【0251】なお、音楽コンテンツ C 及びコンテンツ鍵 K_c ではなく、ストレージ鍵 K_S が破壊されている場合には、包括管理ユニット(X)315の再インストールを行う。この場合であっても、EMDサーバ(X)4-3にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすることができる。

【0252】このように、音楽コンテンツ配信システムでは、例えば、ハードディスクのクラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

【0253】(5) 包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット(X)315とポータブルデバイス(X)6-3との間では、ポータブルデバイス(X)6-3の固有のID及び認証鍵(MG-ID/IK)と、包括管理ユニット(X)315の固有のマスター鍵(OMG-MK)とを用いて、相互認証が行われる。

【0254】包括管理ユニット(X)315とポータブルデバイス(X)6-3との間で、相互認証が行われると、包括管理ユニット(X)315からポータブルデバイス(X)6-3へ音楽コンテンツを送信(チェックアウト)したり、ポータブルデバイス(X)6-3から包括管理ユニット(X)315への音楽コンテンツの返却(チェックイン)をしたりできるようになる。なお、包括管理ユニット(X)315は、パーソナルコンピュータ1のHDD21内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス(X)6-3は、内部のメモリカード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット(X)315からポータブルデバイス(X)6-3へ音楽コンテンツを送信する場合には、パーソナルコンピュータ1のHDD21上の音楽コンテンツが、ポータブルデバイス(X)6-3に装着されたメモリカード上に転送されることとなる。また、ポータブルデバイス(X)6-3から包括管理ユニット(X)315へ音楽コンテンツを送信する場合には、ポータブルデバイス(X)6-3に装着されたメモリカード上の音楽コンテンツが、パーソナルコンピュータ1のHDD21上に転送されることとなる。

【0255】ポータブルデバイス(X)6-3は、ID

情報(MG-ID)、複数世代分の認証鍵(MG-IK)及び複数世代分のマスター鍵(OMG-MK)を工場出荷時から予め保持している。ポータブルデバイス(X)6-3には、後に外部からこれらの鍵等は供給されない。ポータブルデバイス(X)6-3は、必要に応じて、認証鍵(MG-IK)及びマスター鍵(OMG-MK)の世代を更新する。ポータブルデバイス(X)6-3は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス(X)6-3は、第0世代から第99世代の100世代分の認証鍵(MG-IK[0-99])及びマスター鍵(OMG-MK[0-99])を保持しているものとする。なお、第 i 世代の認証鍵を(MG-IK[i])と示し、第 i 世代のマスター鍵を(OMG-MK[i])と示す。

【0256】また、包括管理ユニット(X)315は、マスター鍵(OMG-MK)を保持することによって、オーディオ用コンパクトディスク等からパーソナルコンピュータ1内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット(X)315は、マスター鍵(OMG-MK)を保持することによって、EMDサーバ(X)4-3から音楽コンテンツをダウンロードして、パーソナルコンピュータ1内に保存することができる。

【0257】ここで、包括管理ユニット(X)315では、コンパクトディスクから音楽コンテンツを転送することはできるがEMDサーバ(X)4-3からは音楽コンテンツをダウンロードすることができないマスター鍵(OMG-MK)と、コンパクトディスクからもEMDサーバ(X)4-3からも音楽コンテンツを転送することができるマスター鍵(OMG-MK)とが異なったものとなっている。以下、コンパクトディスクから音楽コンテンツを転送することはできるがEMDサーバ(X)4-3からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからもEMDサーバ(X)4-3からも音楽コンテンツを転送することができる鍵のことをEMD鍵ともいう。

【0258】なお、本例では、第0世代のマスター鍵(OMG-MK[0])がリッピング専用鍵となっており、第1世代以後のマスター鍵(OMG-MK[1~99])がEMD鍵となっている。

【0259】つぎに、リッピング専用鍵を用いた処理の手順について説明する。

【0260】包括管理ユニット(X)315がCD-ROMからインストールされる場合には、図27に示すように、包括管理ユニット(X)315のインストールソフトウェアが格納されたCD-ROM361とともに、ポータブルデバイス(X)6-3と、フロッピー(登録

商標)ディスク362とが例えばセットで販売される。フロッピーディスク362には、ポータブルデバイス(X)6-3のID情報(MG-ID)、第0世代の認証鍵(MG-IK[0])、第0世代のマスター鍵(OMG-MK[0])が格納されている。

【0261】続いて、販売されたポータブルデバイス(X)6-3等を使用可能とするには、まず、CD-ROM361をパーソナルコンピュータ1に装着する(ステップS11)。続いて、このCD-ROM361から包括管理ユニット(X)315をパーソナルコンピュータ1にインストールする(ステップS12)。すると、包括管理ユニット(X)315がパーソナルコンピュータ1のハードディスク内に格納されることとなる(ステップS13)。続いて、フロッピーディスク362に格納されているポータブルデバイス(X)6-3のID情報(MG-ID)と、第0世代の認証鍵(MG-IK[0])と、第0世代のマスター鍵(OMG-MK[0])とをパーソナルコンピュータ1に保存する(ステップS14)。

【0262】このことによって、包括管理ユニット(X)315は、音楽CD363等により提供される音楽コンテンツを、パーソナルコンピュータ1のハードディスク内に格納することができるようになる(ステップS15)。なお、第0世代のマスター鍵(OMG-MK[0])は、リッピング専用鍵なので、EMDサーバ(X)4-3から音楽コンテンツをダウンロードできないようになっている。

【0263】また、ポータブルデバイス(X)6-3は、世代更新がされていく100世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第0世代とされている。このため、第0世代の認証鍵及びマスター鍵を保持している包括管理ユニット(X)315と、ポータブルデバイス(X)6-3との相互認証が可能となる。したがって、音楽CD363等により提供される音楽コンテンツを、ポータブルデバイス(X)6-3のメモリーカードに格納することができるようになる(ステップS16)。

【0264】一方、包括管理ユニット(X)315がネットワークを介して提供される場合には、図28に示すように、ポータブルデバイス(X)6-3とともに、インターネット上のEMD登録サーバ3のアドレス、ユーザID及びパスワード等が提供される。

【0265】続いて、販売されたポータブルデバイス(X)6-3等を使用可能とするには、まず、ユーザID及びパスワードを用いてネットワーク上のEMD登録サーバ3にアクセスをする(ステップS21)。続いて、EMD登録サーバ3は、ユーザID及びパスワードの認証を行う(ステップS22)。続いて、認証に問題がなければ、EMD登録サーバ3は、包括管理ユニット(X)315のインストールソフトウェアと、ポータブ

ルデバイス(X)6-3のID情報(MG-ID)と、第0世代の認証鍵(MG-IK[0])と、第0世代のマスター鍵(OMG-MK[0])とを、パーソナルコンピュータ1に送信する(ステップS23)。続いて、パーソナルコンピュータ1は、包括管理ユニット(X)315のインストールソフトウェアを起動して、包括管理ユニット(X)315をインストールするとともに、ポータブルデバイス(X)6-3のID情報(MG-ID)と、第0世代の認証鍵(MG-IK[0])と、第0世代のマスター鍵(OMG-MK[0])とをHDD21に保存する(ステップS24)。すると、ハードディスクには、包括管理ユニット(X)315が格納されることとなる(ステップS25)。

【0266】このことによって、包括管理ユニット(X)315は、音楽CD363等により提供される音楽コンテンツを、パーソナルコンピュータ1のHDD21内に格納することができるようになる(ステップS26)。なお、第0世代のマスター鍵(OMG-MK[0])は、リッピング専用鍵なので、EMDサーバ(X)4-3から音楽コンテンツをダウンロードできないようになっている。

【0267】また、ポータブルデバイス(X)6-3は、世代更新がされていく100世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第0世代とされている。このため、第0世代の認証鍵及びマスター鍵を保持している包括管理ユニット(X)315と、ポータブルデバイス(X)6-3との相互認証が可能となる。したがって、音楽CD363等により提供される音楽コンテンツを、ポータブルデバイス(X)6-3のメモリーカード内に格納することができるようになる(ステップS27)。

【0268】なお、以上の図27及び図28に示した方法に限られず、包括管理ユニット(X)315及びリッピング専用の第0世代のマスター鍵(OMG-MK[0])をCD-ROM361に格納しておき、ポータブルデバイス(X)6-3との認証用のID及び第0世代の認証鍵(MG-ID/IK)をネットワークを介して提供しても良い。

【0269】つぎに、リッピング専用鍵をEMD鍵に鍵に更新して、EMDサーバ(X)4-3からダウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。

【0270】包括管理ユニット(X)315は、図27又は図28に示した手順により、CD-ROM等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パーソナルコンピュータ1内のHDD21にインストールされている。このとき包括管理ユニット(X)315は、リッピング専用である第0世代のマスター鍵(OMG-MK[0])と、認証用のID及び第0世代の認証鍵(MG-ID/IK[0])とを保

持しており、ポータブルデバイス(X) 6-3の鍵の世代もデフォルトのままである。

【0271】まず、パーソナルコンピュータ1は、図29に示すように、ユーザID及びパスワードを用いてネットワーク上のEMD登録サーバ3にアクセスをする(ステップS31)。続いて、EMD登録サーバ3は、ユーザID及びパスワードの認証を行う(ステップS32)。続いて、認証に問題がなければ、EMD登録サーバ3は、パーソナルコンピュータ1のID情報(OMG-ID)を登録し、包括管理ユニット(X) 315がEMDサーバ(X) 4-3と接続するための公開鍵(OMG-PK)、秘密鍵(OMG-KS)及び公開鍵の認証書(Cert[PK])を生成する(ステップS33)。続いて、EMD登録サーバ3は、生成した公開鍵(OMG-PK)、秘密鍵(OMG-KS)及び公開鍵の認証書(Cert[PK])を、パーソナルコンピュータ1に送信する(ステップS34)。

【0272】続いて、EMD登録サーバ3は、ポータブルデバイス(X) 6-3のID情報(MG-ID)、第i世代の認証鍵(MG-IK[i])、第i世代のマスター鍵(OMG-MK[i])をパーソナルコンピュータ1に送信する(ステップS35)。続いて、パーソナルコンピュータ1の包括管理ユニット(X) 315は、受信したID情報(MG-ID)、第i世代の認証鍵(MG-IK[i])、第i世代のマスター鍵(OMG-MK[i])に基づき、これらの鍵を第i世代に世代更新する(ステップS36)。続いて、包括管理ユニット(X) 315は、ポータブルデバイス(X) 6-3との間で認証を行う(ステップS37)。ポータブルデバイス(X) 6-3は、認証がされると、自己の鍵の世代を第i世代に更新する(ステップS38)。

【0273】このことによって、包括管理ユニット(X) 315は、音楽CD363等により提供される音楽コンテンツを、パーソナルコンピュータ1のハードディスク内に格納することができるとともに、EMDサーバ(X) 4-3からダウンロードした音楽コンテンツをパーソナルコンピュータ1のHDD21に格納することができるようになる。

【0274】つぎに、EMD鍵等の世代更新をする手順について説明する。

【0275】包括管理ユニット(X) 315は、第i世代のマスター鍵(OMG-MK[i])と、認証用のID及び第0世代の認証鍵(MG-ID/IK[i])とを保持しており、ポータブルデバイス(X) 6-3の鍵の世代も第i世代となっている。

【0276】まず、図30に示すように、パーソナルコンピュータ1が何らかの処理のため、EMD登録サーバ3にアクセスすると、EMD登録サーバ3は、包括管理ユニット(X) 315のIDを認証して、第(i+k)世代の認証鍵(MG-IK[i+k])及び第(i+

k)世代のマスター鍵(OMG-MK[i+k])をパーソナルコンピュータ1に送信する(ステップS41)。続いて、パーソナルコンピュータ1の包括管理ユニット(X) 315は、受信した認証鍵及びマスター鍵を、第(i+k)世代に更新する(ステップS42)。続いて、包括管理ユニット(X) 315は、ポータブルデバイス(X) 6-3と認証を行う(ステップS43)。ポータブルデバイス(X) 6-3は、認証がされると、自己の鍵の世代を第i世代から第(i+k)世代に更新する(ステップS44)。

【0277】また、図31に示すように、一方、ポータブルデバイス(X) 6-3が用いている認証鍵等の世代が第(i+k)世代となっており、包括管理ユニット(X) 315が保持している認証鍵等の世代が第i世代となっている場合には、ポータブルデバイス(X) 6-3と包括管理ユニット(X) 315との認証が行われると、認証失敗となる(ステップS51)。認証を失敗すると、包括管理ユニット(X) 315は、EMD登録サーバ3に対して、鍵要求を行う(ステップS52)。鍵要求があると、EMD登録サーバ3は、包括管理ユニット(X) 315のIDを認証して、第(i+k)世代の認証鍵(MG-IK[i+k])及び第(i+k)世代のマスター鍵(OMG-MK[i+k])を送信する(ステップS53)。続いて、包括管理ユニット(X) 315は、受信した認証鍵及びマスター鍵を、第(i+k)世代に更新する(ステップS54)。続いて、包括管理ユニット(X) 315は、ポータブルデバイス(X) 6-3と認証を行う(ステップS55)。

【0278】このことによって、包括管理ユニット(X) 315は、音楽CD363等により提供される音楽コンテンツを、パーソナルコンピュータ1のハードディスク内に格納することができるとともに、EMDサーバ(X) 4-3からダウンロードした音楽コンテンツをパーソナルコンピュータ1のHDD21に格納することができるようになる(ステップS38)。

【0279】以上のように、音楽コンテンツ配信システムでは、包括管理ユニット(X) 315及びポータブルデバイス(X) 6-3が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システムでは、サーバから配信された音楽コンテンツの安全性が高まり、例えば、リッピング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

【0280】また、音楽コンテンツ配信システムでは、包括管理ユニット(X) 315及びポータブルデバイス(X) 6-3が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット(X) 315は、マスター鍵及び認証鍵がネットワークを介し

て供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

【0281】

【発明の効果】本発明によれば、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元又は再配信されたコンテンツデータの再生及び／又は制御を行う。

【0282】このことにより、本発明では、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態の音楽コンテンツ配信システムの構成を示す図である。

【図2】上記音楽コンテンツ配信システムにおけるパーソナルコンピュータの構成を示す図である。

【図3】上記音楽コンテンツ配信システムにおけるポータブルデバイスの構成を示す図である。

【図4】上記パーソナルコンピュータの機能について説明する図である。

【図5】表示操作指示ウィンドウの一例を示す図である。

【図6】録音プログラムがディスプレイに表示させる表示例を示す図である。

【図7】上記音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて説明するための図である。

【図8】統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図である。

【図9】一般的に用いられる利用条件情報のフォーマットを説明する図である。

【図10】包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。

【図11】上記統一利用条件情報のオートマトンファイルの構成を説明する図である。

【図12】上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。

【図13】上記オートマトンをtuple列で表現した図である。

【図14】上記オートマトン記述部の構成を説明する図

である。

【図15】XMLの仕様に基づいて規定されたDTDで定義されているイベントとコマンドとを示す図である。

【図16】上記オートマトン記述部の第1の記述例を示す図である。

【図17】上記第1の記述例の状態遷移図である。

【図18】上記オートマトン記述部の第2の記述例を示す図である。

【図19】上記第2の記述例の状態遷移図である。

【図20】上記オートマトン記述部の第3の記述例を示す図である。

【図21】上記第3の記述例の状態遷移図である。

【図22】上記オートマトン記述部の第4の記述例を示す図である。

【図23】上記統一利用条件情報のパラメータファイルの構成を説明する図である。

【図24】上記パラメータファイルを更新した場合の構成を説明する図である。

【図25】上記パラメータファイルのパラメータ記述部の構成を説明する図である。

【図26】上記包括管理ユニットによるコンテンツの管理方法について説明する図である。

【図27】包括管理ユニットがCD-ROMからインストールされる場合の処理手順について説明する図である。

【図28】包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。

【図29】リッピング鍵からEMD鍵に更新する更新手順について説明する図である。

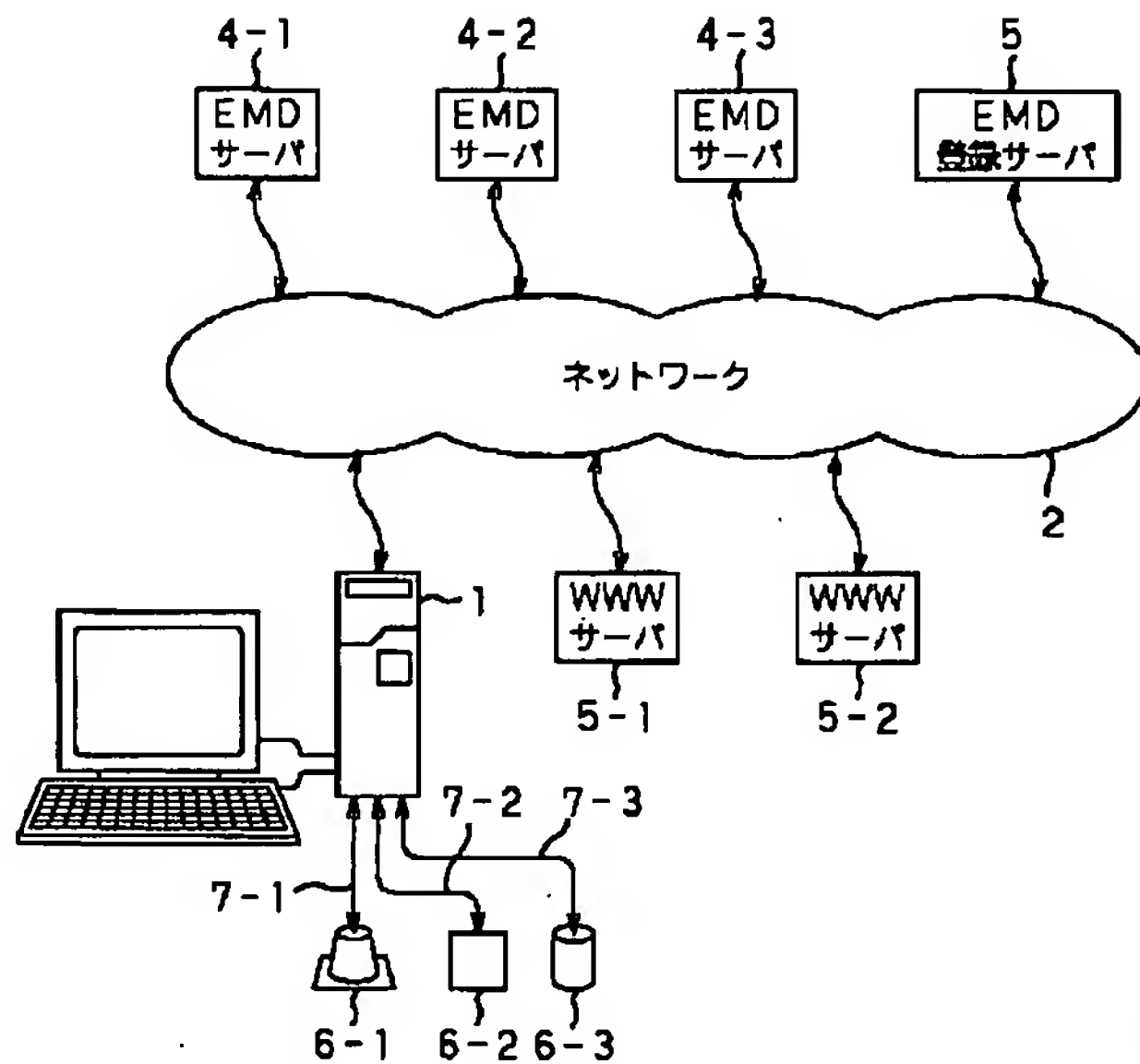
【図30】EMD鍵を更新する手順の第1の例について説明する図である。

【図31】EMD鍵を更新する手順の第2の例について説明する図である。

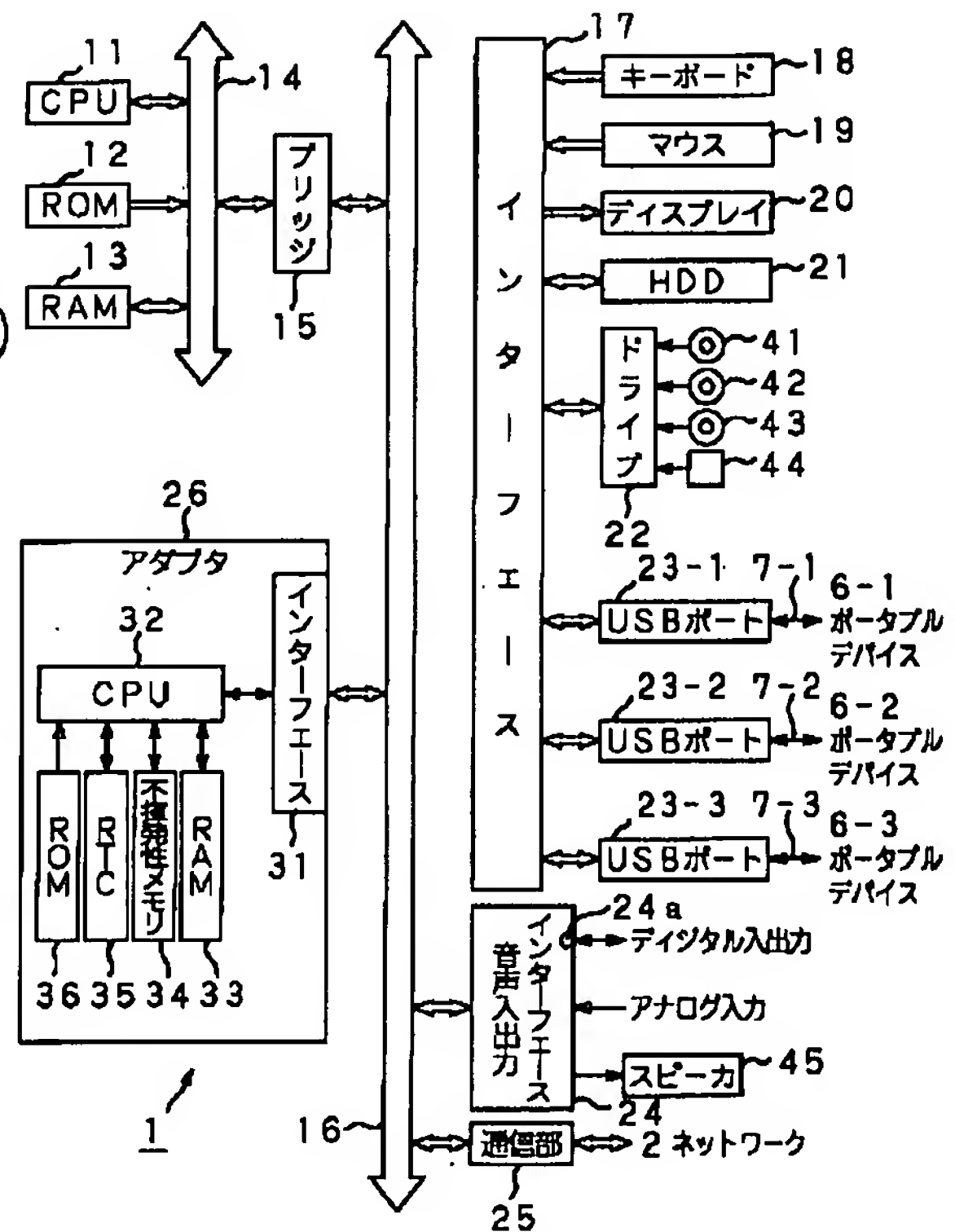
【符号の説明】

1 パーソナルコンピュータ、2 ネットワーク、3 EMD登録サーバ、4 EMDサーバ、6 ポータブルデバイス、7 USBインターフェース、21ハードディスク、311、312 再生用アプリケーション、313、314デバイスドライバ、315 包括管理ユニット、316 EMD用受信インターフェース、317 EMD用送信インターフェース、318 PDドライバ

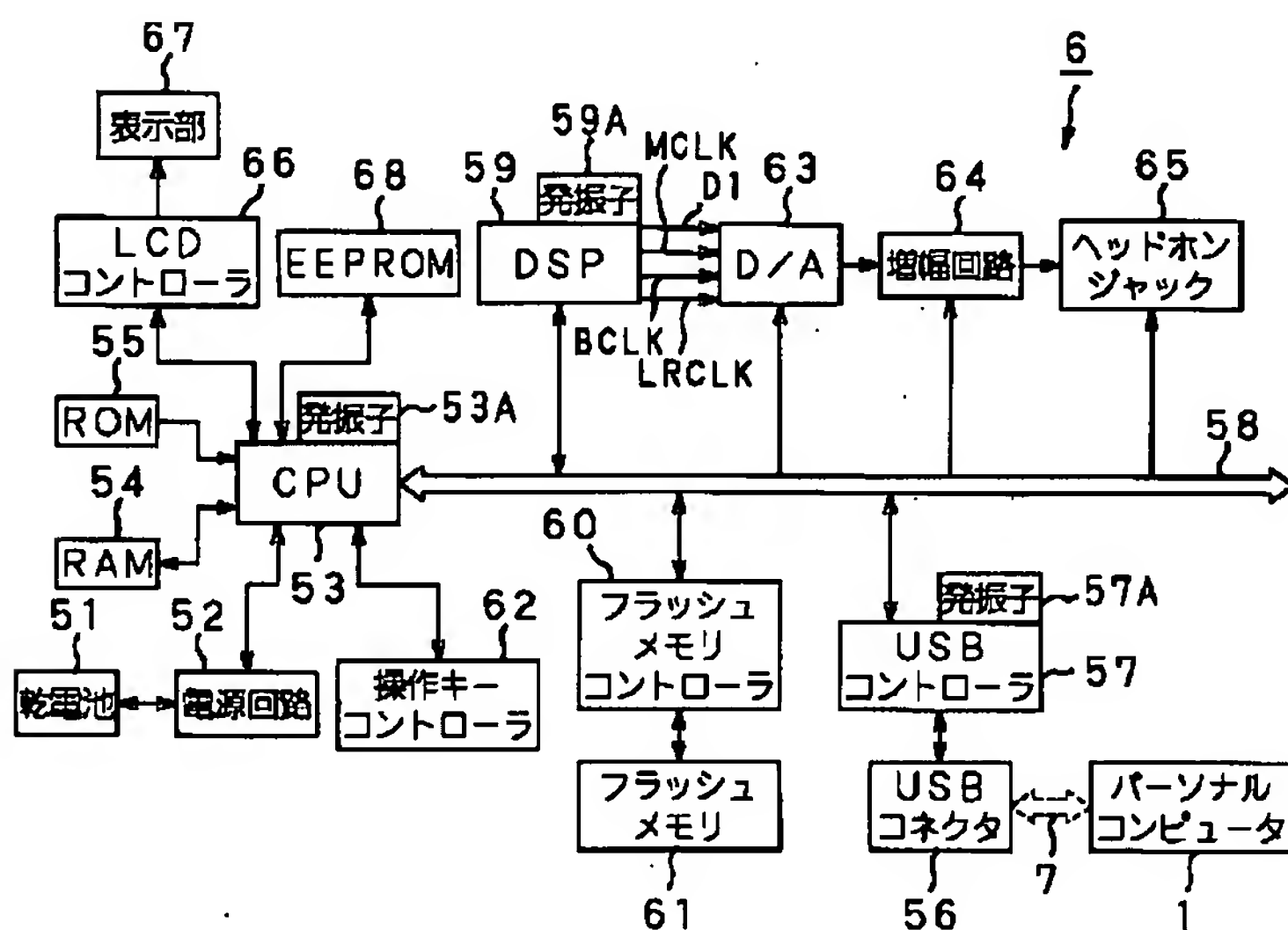
【図1】



【図2】



【図3】



【図9】

(a)

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

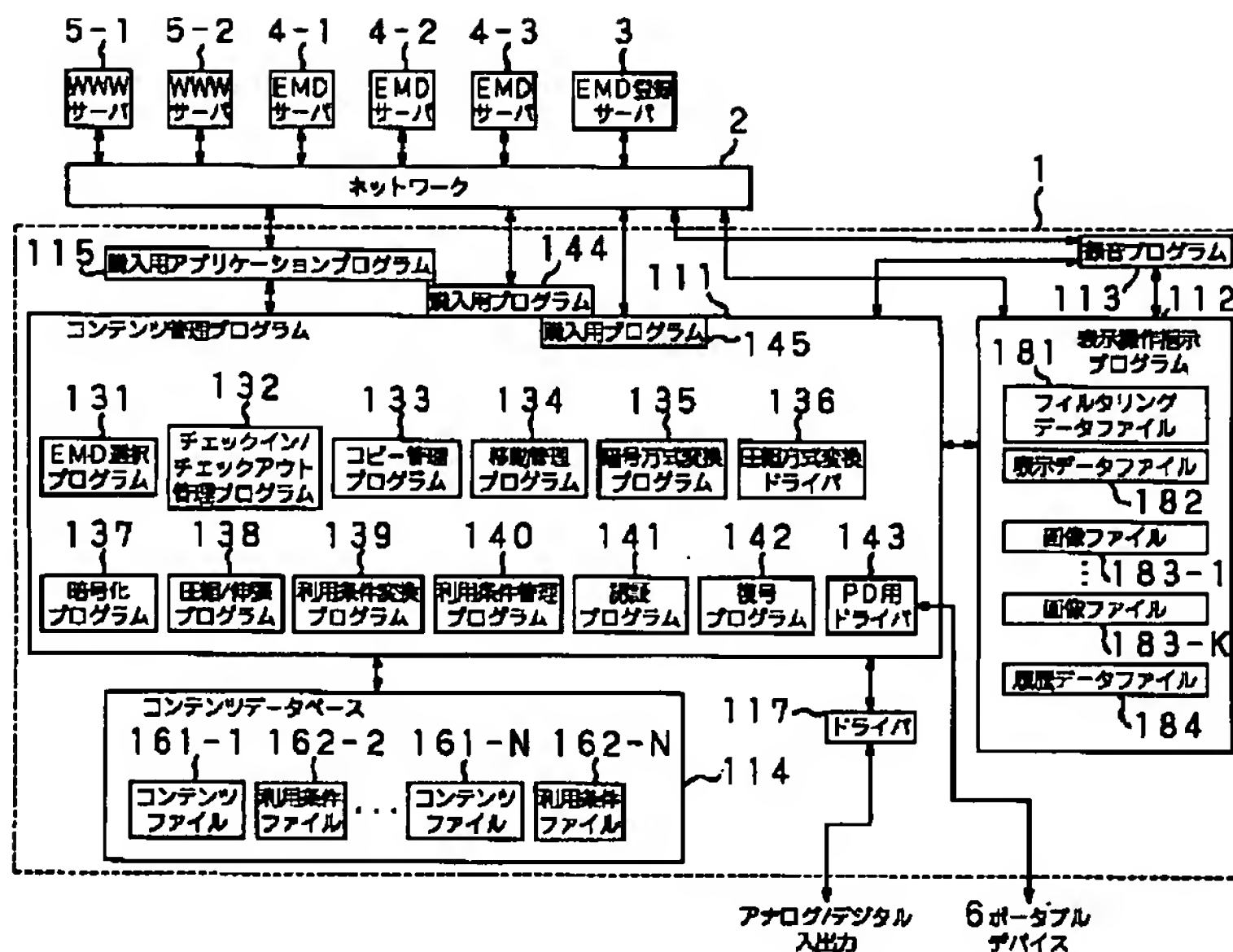
(b)

コンテンツ
利用条件情報

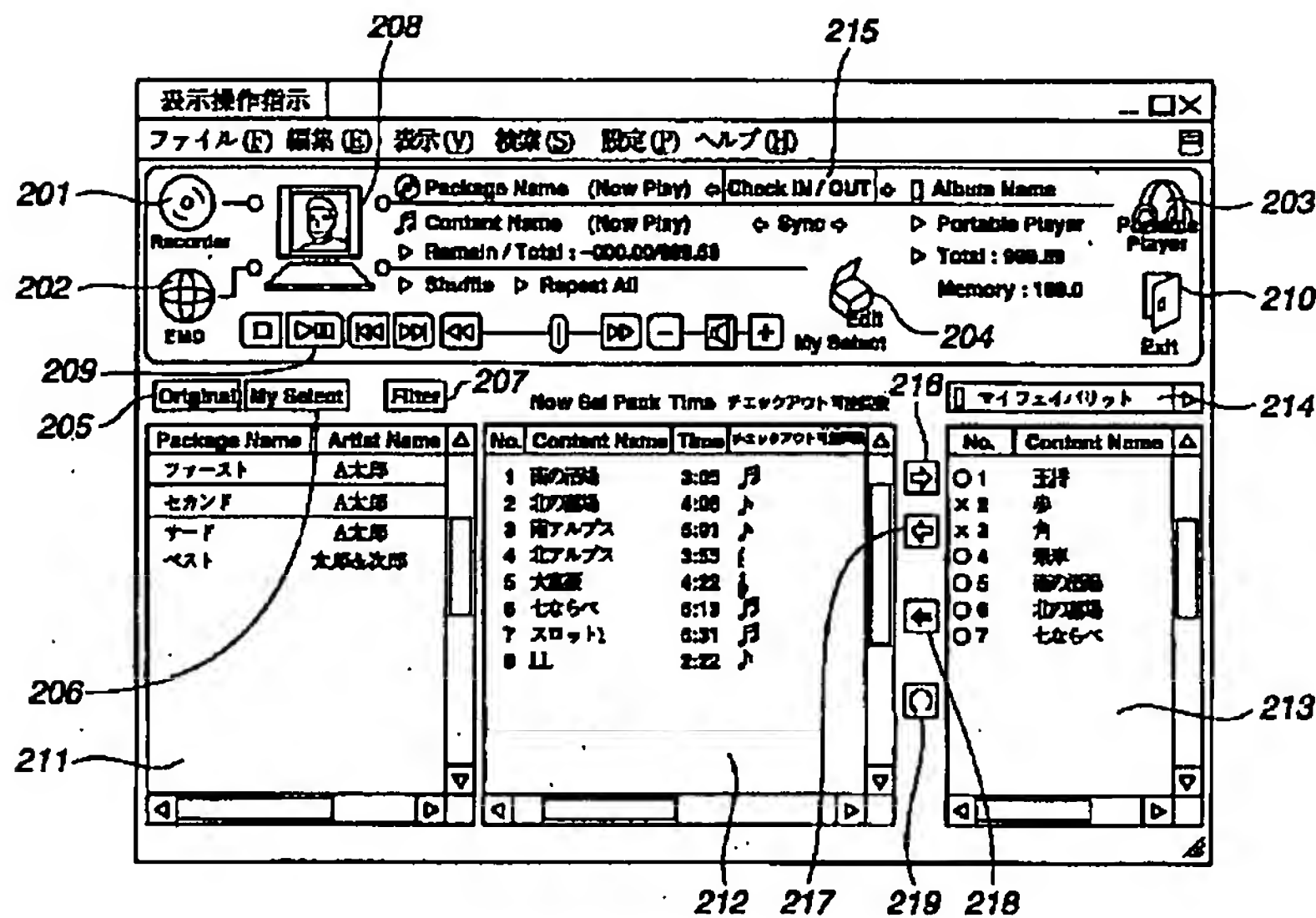
【図10】

インデックスファイル	~331
オートマトンファイル	~332
パラメータファイル	~333
履歴ファイル	~334

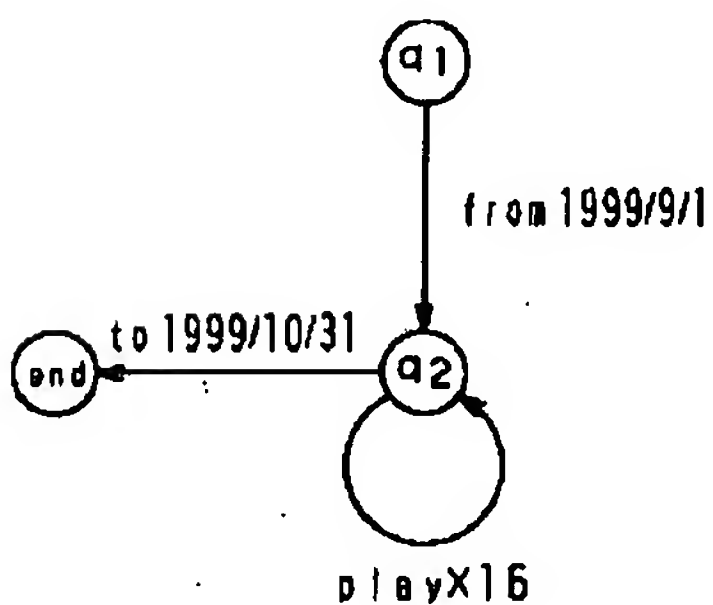
【図4】



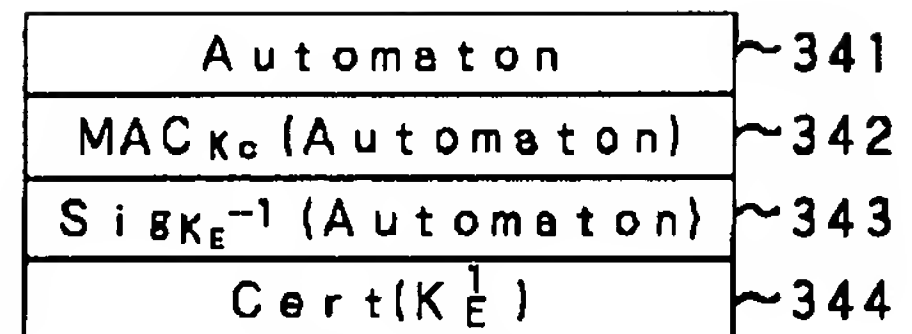
【図5】



【図21】



【図11】



【図13】

```

(q1, pay10, q2)
(q1, a.pay1000, q3)
(q1, pay(10xn), q4)
(q2, play, q1)
(q3, play, q3)
(q4, playxn, q4)
(q4, ε, q1)
(q5, pay100, q6)
(q5, a.pay2000, q7)
(q6, copy, q5)
(q7, copy, q7)
(q8, play, q8)
(q8, copy, q9)

```

【図15】

```

(!ENTITY% event" (
  play
  copy
  pay-for-play
  pay-for-copy
  pay-for-album-play
  pay-for-album-copy
  from
  to
  null
) ")

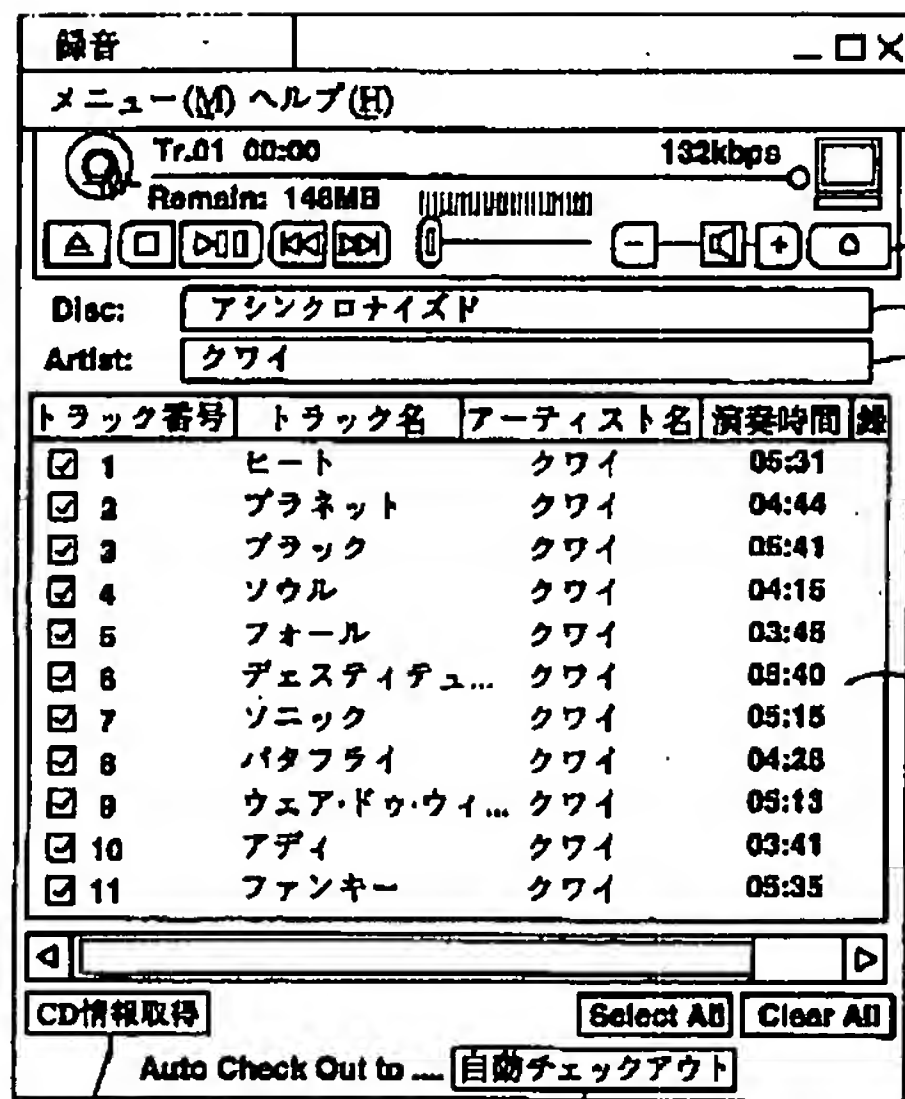
```

```

(!ENTITY% command" (
  drop
  dup
  swap
  add
  subtract
  multiply
  divide
  remainder
  upper
  lower
  equal
  less
  greater
  less-equal
  greater-equal
  and
  or
  not
  bit-and
  bit-or
  bit-xor
  bit-not
) ")

```

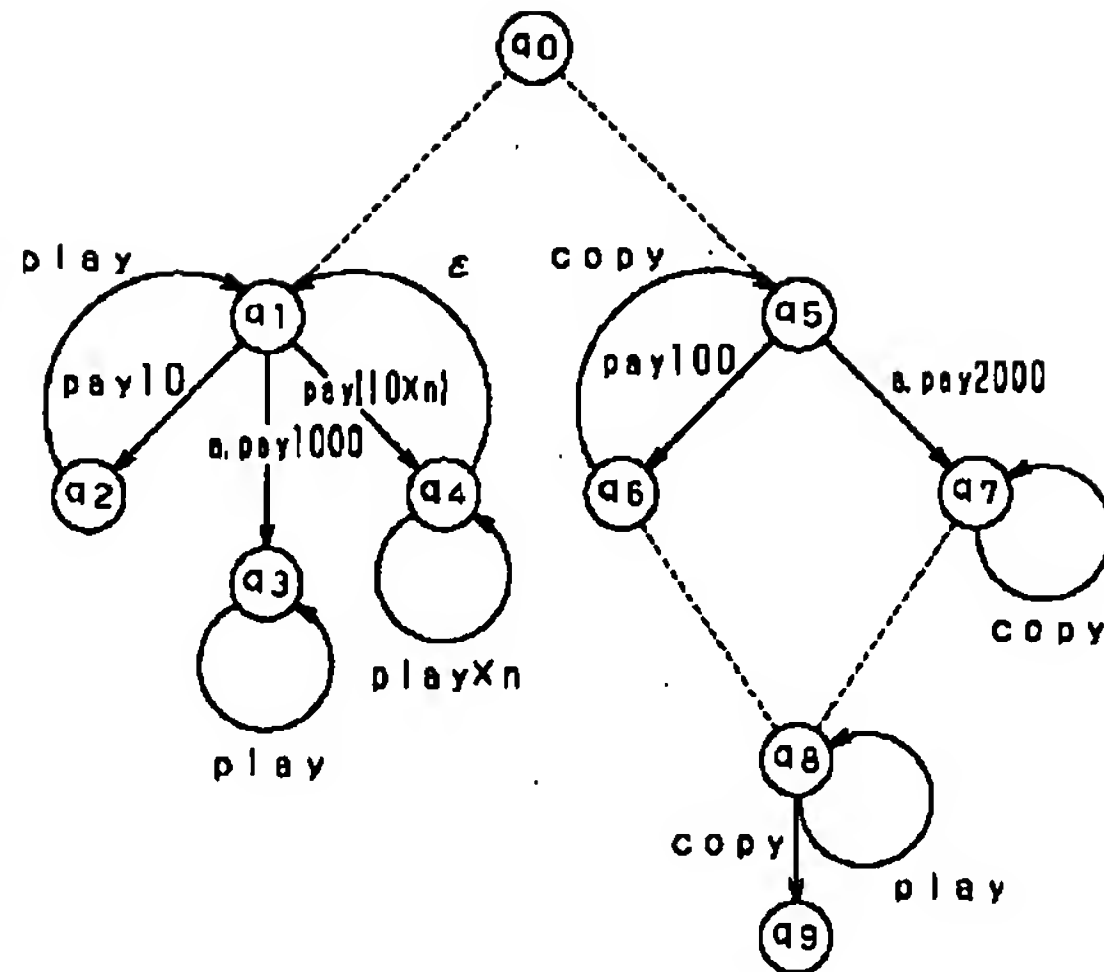
【図6】



254

255

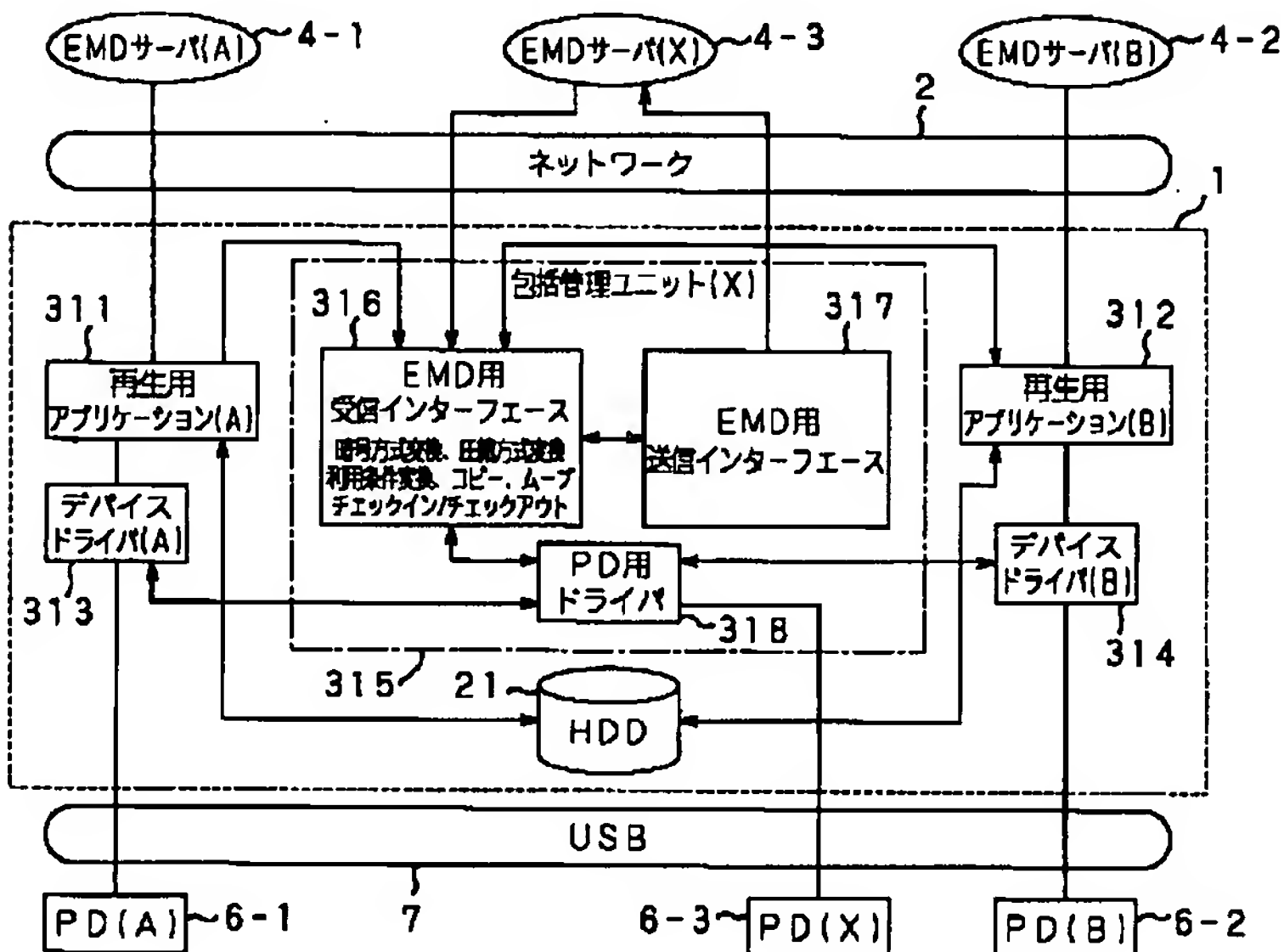
【図12】



【図17】

【図19】

【図7】

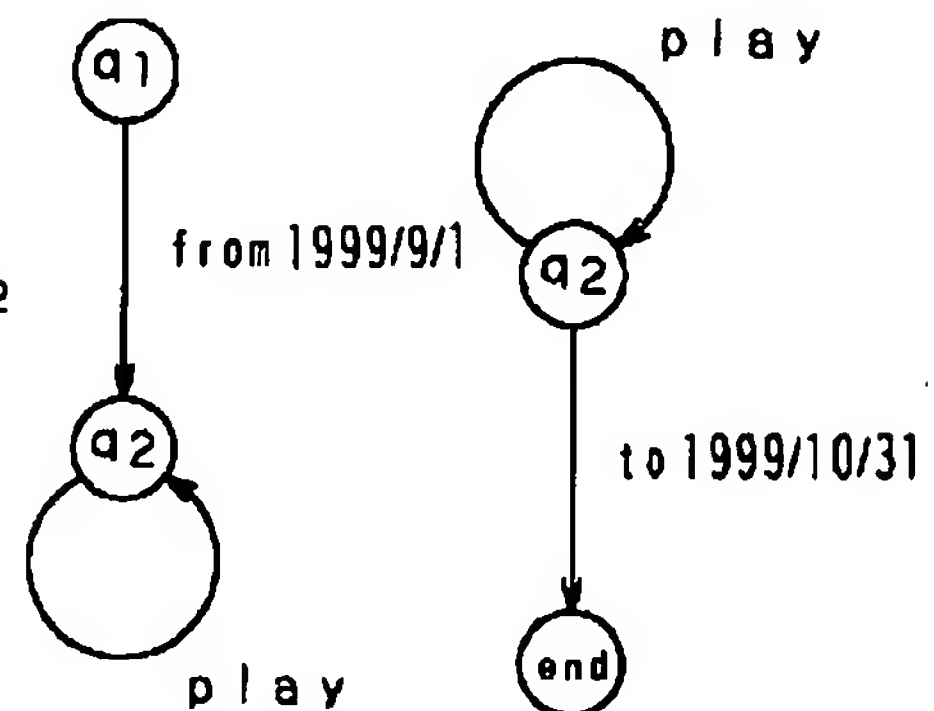


【図23】

【図24】

Parameters	~ 351
MAC _{K_c} (Parameters)	~ 352
Sig _{K_E} ⁻¹ (Parameters)	~ 353
Cert(K _E ¹)	~ 354

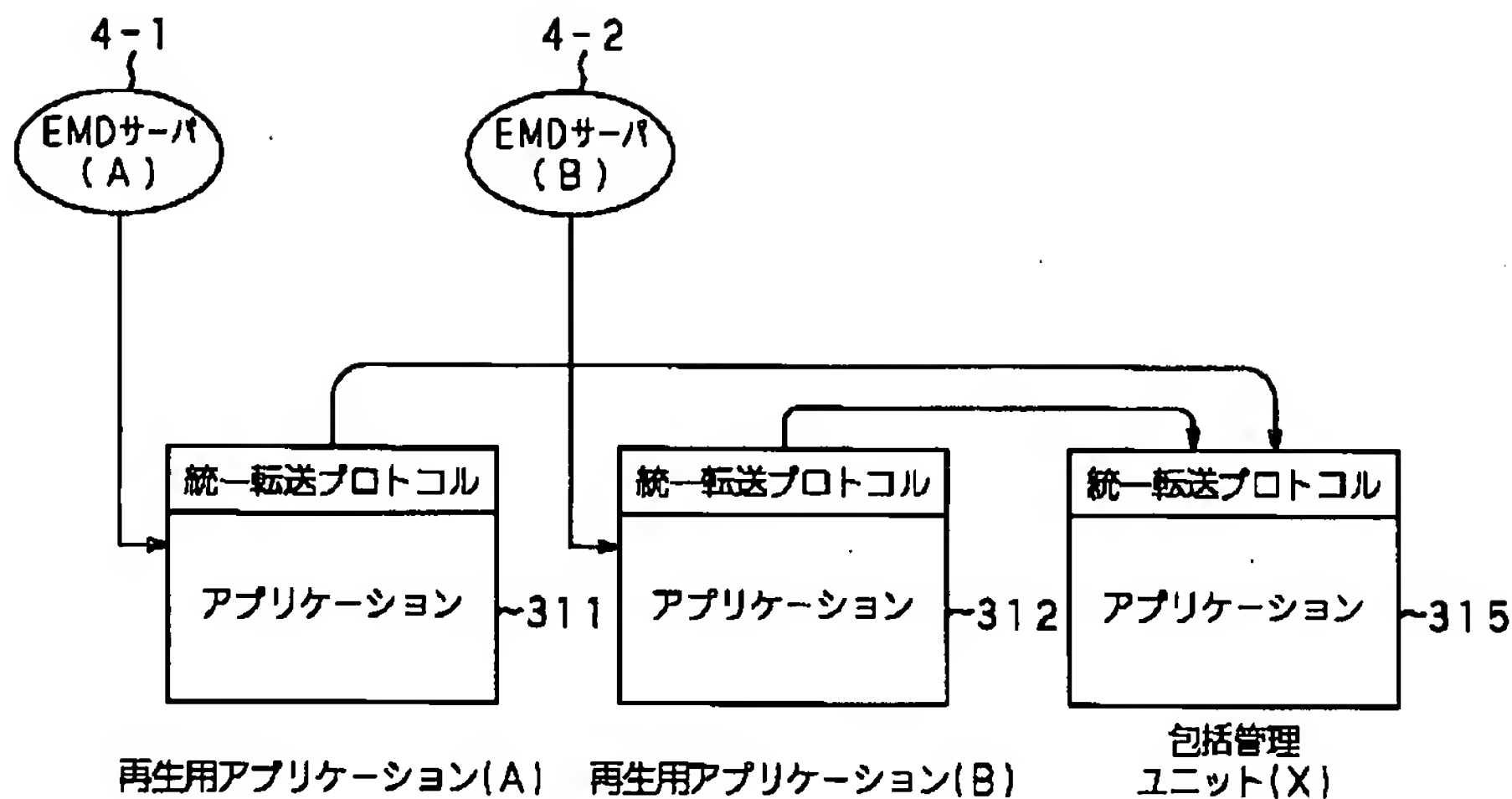
Parameters	~ 351
Entity ID	~ 355
MAC _{K_c} (Parameters)	~ 352
Sig _{K_E} ⁻¹ (Parameters)	~ 353
Cert(K _E ¹)	~ 354



【図25】

Entity ID	~ 356
Contents ID	~ 357
Contents	~ 358

【図8】



【図14】

Entity ID	~345
Content ID	~346
Automaton Version	~347
Variables	~348
Tuples	~349
Automaton Version	~347
Variables	~348
Tuples	~349
:	

【図18】

【図16】

Content playable from 1999/9/1

```

(automaton)
  (!--This usage rule system has one Right Unit.
  Initial state is q1-->
  <initial-right-unit state="q1"/>

  (node state="q1")
    (!--If after 1999/9/1, transfer to q2-->
    <rule event="from" next-state="q2">
      (arguments)
        (integer value="time:19990901"/>
      </arguments>
    </rule>
  </node>

  (node state="q2")
    (!--Playable-->
    <rule event="play" next-state="q2"/>
  </node>
</automaton>

```

【図26】

Content playable until 1999/10/31

```

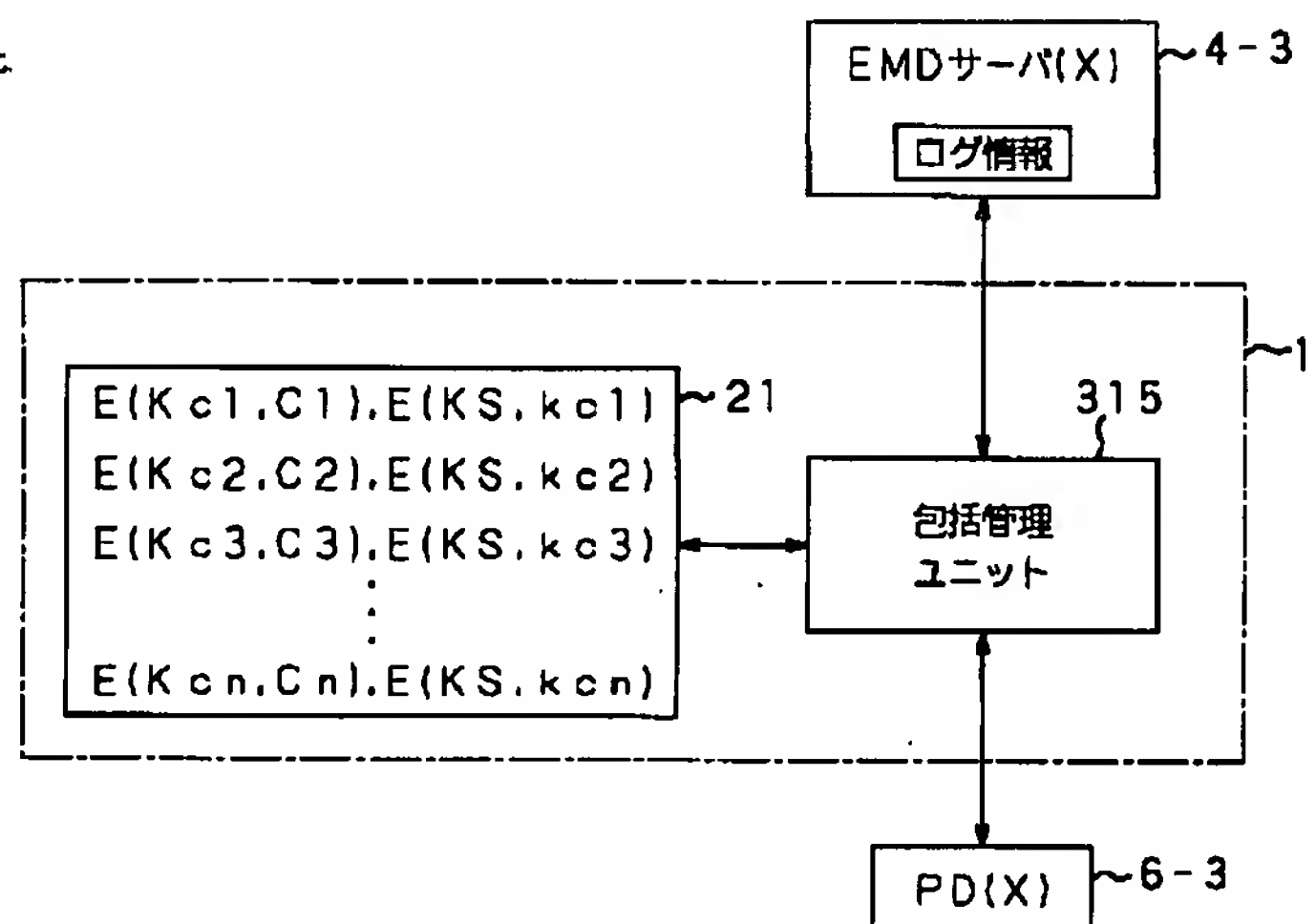
(automaton)
  (!--This Usage Rule System has one Right Unit.
  Initial state is q2-->
  <initial-right-unit state="q2"/>

  (node state="q2")
    (!--If after 1999/10/31, transfer to end-->
    <rule event="to" next-state="end">
      (arguments)
        (integer value="time:19991031"/>
      </arguments>
    </rule>

    (!--Playable-->
    <rule event="play" next-state="q2">
    </rule>
  </node>

  (!--Unusable state-->
  <node state="end"/>
</automaton>

```



【図20】

Content playable 16times 1999/9/1 to 1999/10/31

```

(automaton)
  (!-Define counter variables for playable numbers. Initial value is 16-)
  (define-variable name="count" initial-value="16"/>)

  (!-This Usage Rule System has one Right Unit. Initial state is q1-)
  (initial-right-unit state="q1"/>)

  (node state="q1")
    (!-From 1999/9/1 transfer to q2-)
    (rule event="from" next-state="q2")
    (arguments)
      (integer value="time:19990901"/>)
    (/arguments)
  (/rule)
  (/node)

  (node state="q2")
    (!-From 1999/10/31 transfer to end-)
    (rule event="to" next-state="end")
    (arguments)
      (integer value="time:19991031"/>)
    (/arguments)
  (/rule)

  (rule event="play" next-state="q2")
    (!-playable only for "count" numbers-)
    (arguments)
      (variable name="count"/>)
      (command name="load"/>)
    (/arguments)
    (!-If this rule is selected, the "count" number decrements by one-)
    (action)
      (variable name="count"/>)
      (command name="load"/>)
      (integer value="1"/>)
      (command name="subtract"/>)
      (variable name="count"/>)
      (command name="store"/>)
    (/action)
  (/rule)
  (/node)

  (!-Unusable state-)
  (node state="end"/>)
  (/node)
  (/automaton)

```

【図22】

Content playable less than and/or equal to 16times

```

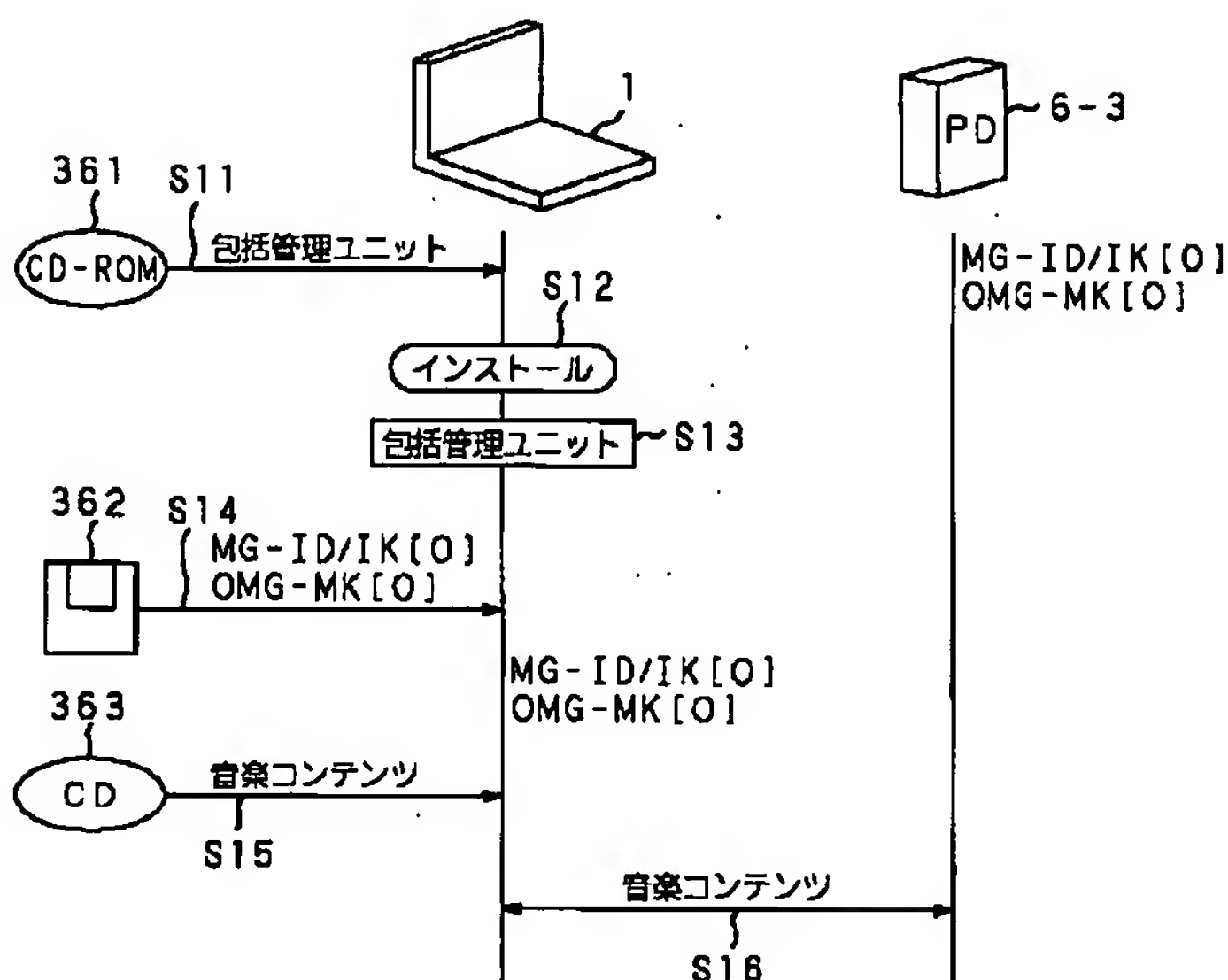
(automaton)
  (!-Define valuable counter for playable numbers
  Initial value is 16-)
  (define-variable name="count" initial-value="16"/>)

  (!-Usage Rule System has one Right Unit
  Initial state is q2-)
  (initial-right-unit state="q1"/>)

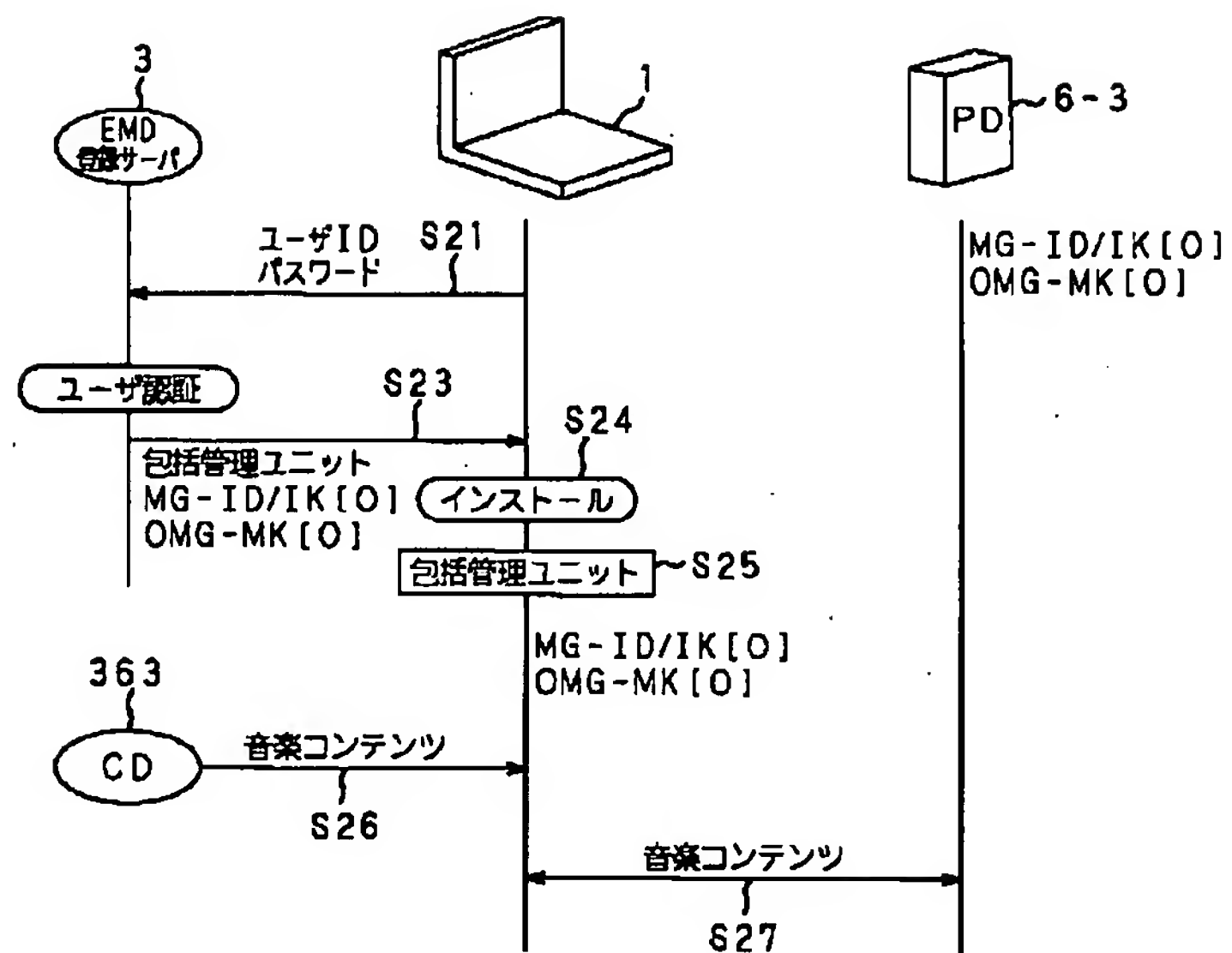
  (node state="q2")
    (rule event="play" next-state="q2")
    (!-Count number of times playable-)
    (arguments)
      (variable name="count"/>)
      (command name="load"/>)
    (/arguments)
    (!-If this rule is selected, "count"
    number decrements by one-)
    (action)
      (variable name="count"/>)
      (command name="load"/>)
      (integer value="1"/>)
      (command name="subtract"/>)
      (variable name="count"/>)
      (command name="store"/>)
    (/action)
  (/rule)
  (/node)
  (/automaton)

```

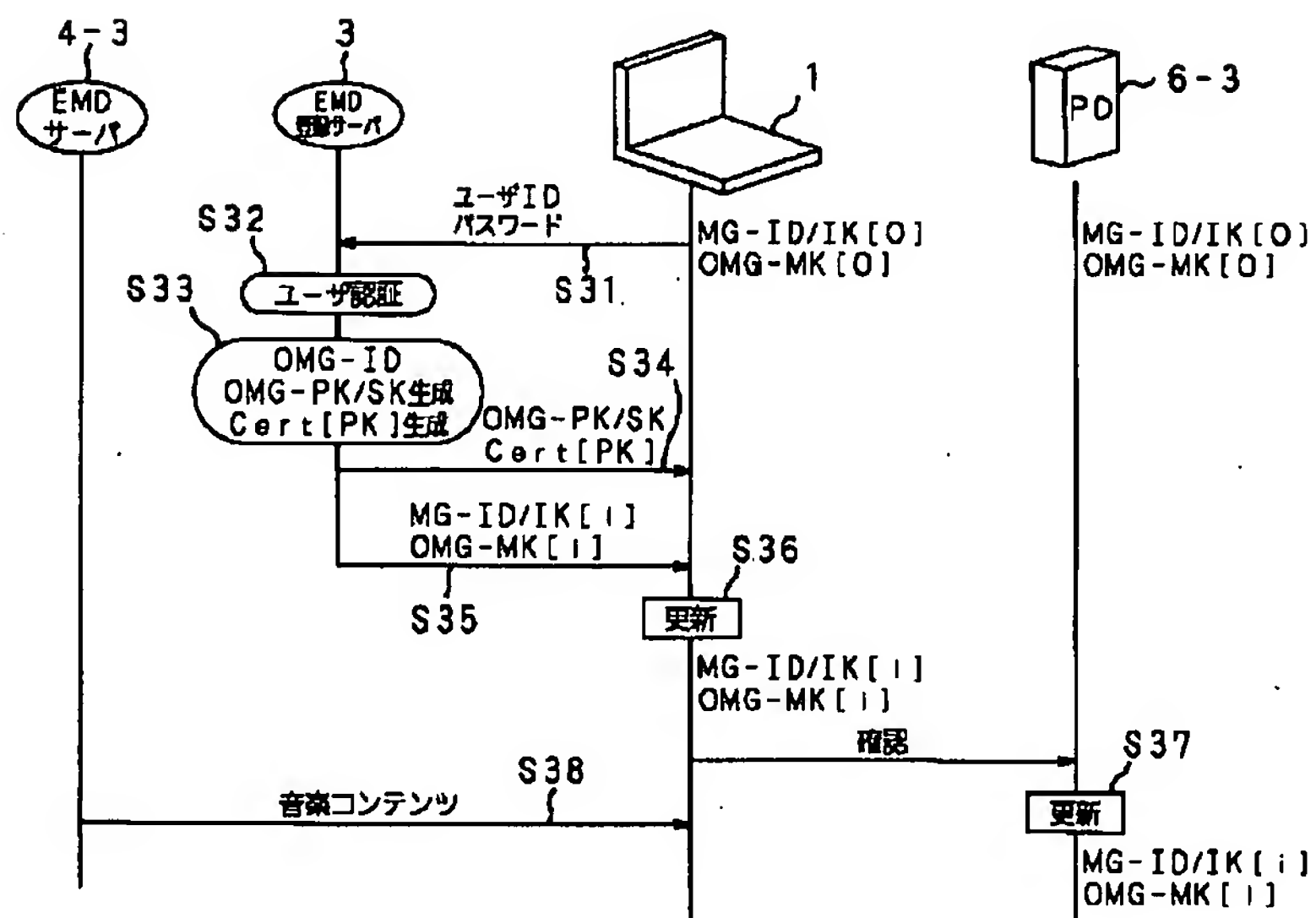
【図27】



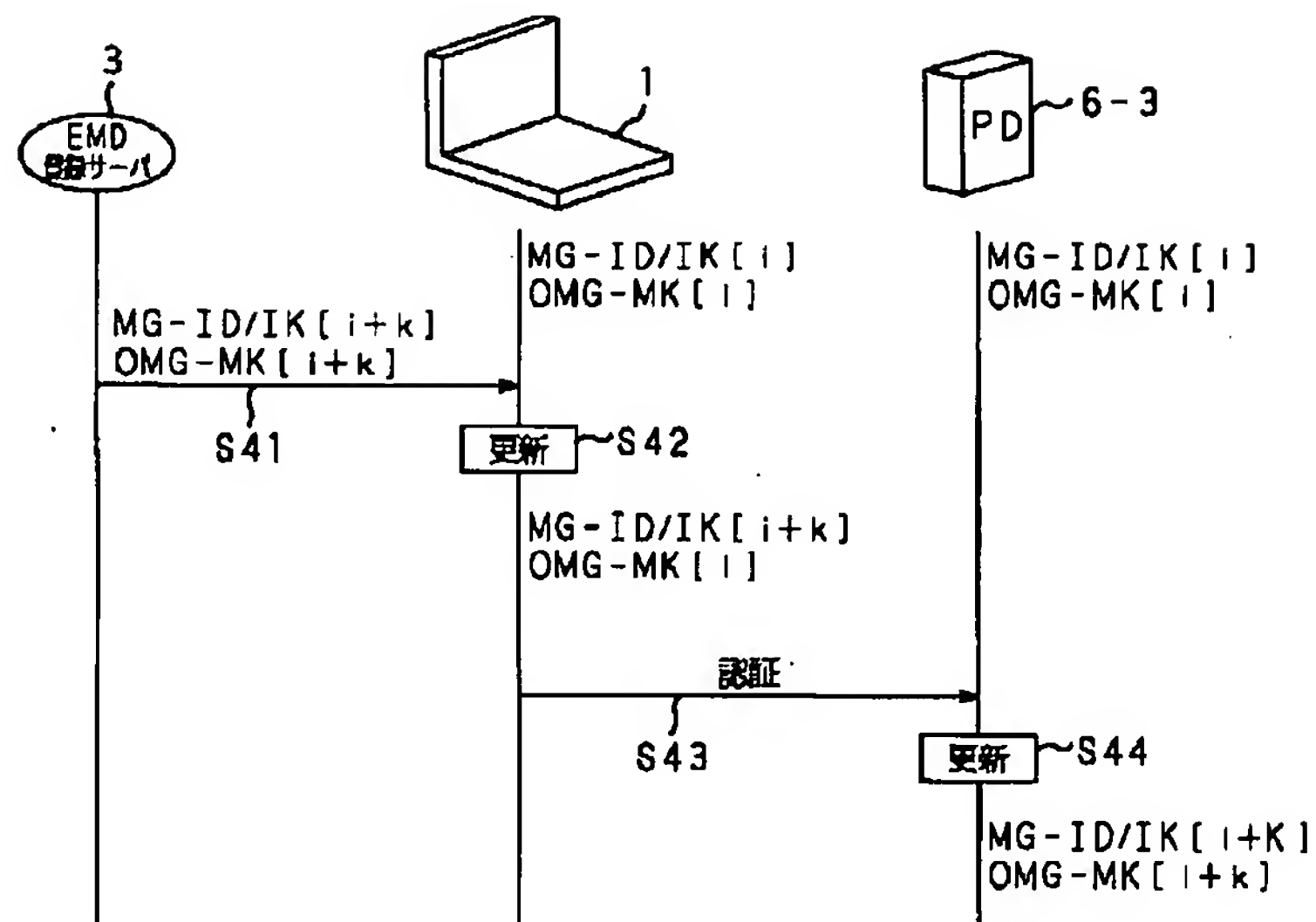
【図28】



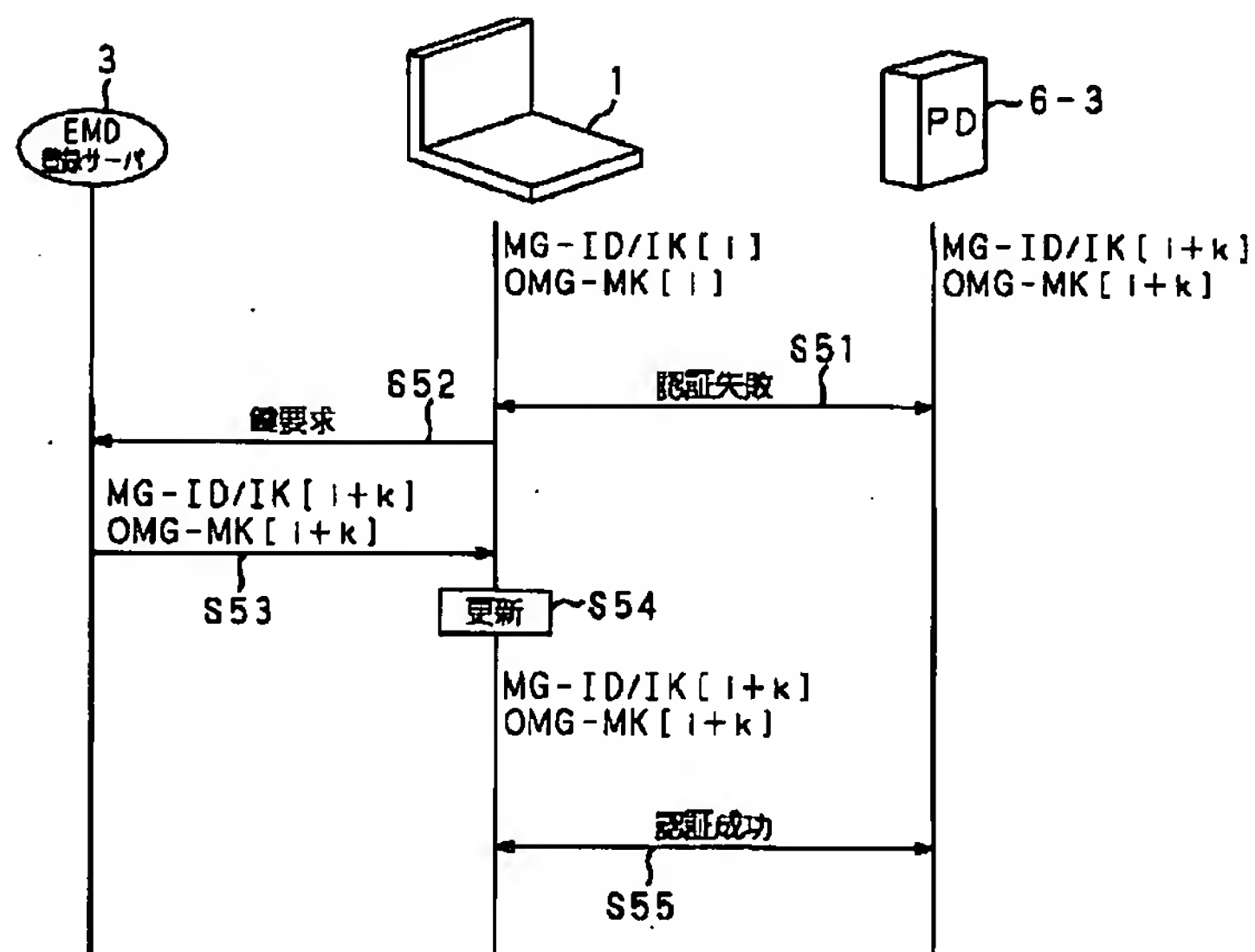
【図29】



【図30】



【図31】



フロントページの続き

(72)発明者 田辺 充
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 江面 裕一
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 佐藤 一郎
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 海老原 宗毅
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

【公報種別】 特許法第 17 条の 2 の規定による補正の掲載

【部門区分】 第 6 部門第 3 区分

【発行日】 平成 19 年 5 月 24 日 (2007. 5. 24)

【公開番号】 特開 2001-195509 (P2001-195509A)

【公開日】 平成 13 年 7 月 19 日 (2001. 7. 19)

【出願番号】 特願 2000-326125 (P2000-326125)

【国際特許分類】

G06Q 30/00 (2006.01)

G10K 15/02 (2006.01)

【F I】

G06F 17/60 302 E

G10K 15/02

【手続補正書】

【提出日】 平成 19 年 3 月 28 日 (2007. 3. 28)

【手続補正 1】

【補正対象書類名】 明細書

【補正対象項目名】 発明の名称

【補正方法】 変更

【補正の内容】

【発明の名称】 コンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コンテンツサーバ

【手続補正 2】

【補正対象書類名】 明細書

【補正対象項目名】 特許請求の範囲

【補正方法】 変更

【補正の内容】

【特許請求の範囲】

【請求項 1】 コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、

上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること

を特徴とするコンテンツ提供システム。

【請求項 2】 コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、

上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること

を特徴とするコンテンツ提供システム。

【請求項3】 コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、

上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、

上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、

上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、

上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、

上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること

を特徴とするコンテンツ配信方法。

【請求項4】 コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、

上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、

上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、

上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、

上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、

上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること

を特徴とするコンテンツ配信方法。

【請求項5】 データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、

上記再生制御プログラムは、

上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、

上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること

を特徴とする記憶媒体。

【請求項6】 データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、

上記再生制御プログラムは、

上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、

、

上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること

を特徴とする記憶媒体。

【請求項7】 コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、

上記コンテンツサーバとの間でデータを送受信する通信手段と、

コンテンツデータを記憶する記憶手段と、

上記記憶手段に記憶されたコンテンツデータを再生する再生手段と、

上記記憶手段に記憶されたコンテンツデータのコンテンツIDリストを含むログ情報を管理し、上記コンテンツサーバへ上記ログ情報を上記通信手段が送信するよう制御し、上記再生手段が上記コンテンツデータを再生するよう制御する制御手段と

を有し、

上記記憶手段に記憶された上記コンテンツデータが上記再生手段で再生できなくなったときは、上記通信手段が上記ログ情報に基づいて上記コンテンツサーバが送信するデータを受信すること

を特徴とするデータ処理装置。

【請求項8】 上記コンテンツサーバが送信するデータは、コンテンツデータであり、上記再生手段は、上記通信手段が受信したコンテンツデータを再生することを特徴とする請求項7記載のデータ処理装置。

【請求項9】 上記コンテンツデータは、コンテンツ鍵で暗号化されており、上記記憶手段は、コンテンツを暗号化したコンテンツ鍵を記憶しており、上記再生手段は上記コンテンツデータを上記コンテンツ鍵で復号化して再生し、上記コンテンツサーバが送信するデータは、コンテンツ鍵であることを特徴とする請求項7記載のデータ処理装置。

【請求項10】 上記制御手段は、上記記憶手段に記憶されたコンテンツデータのバックアップデータを記録媒体に記憶するよう制御することを特徴とする請求項7記載のデータ処理装置。

【請求項11】 上記通信手段は、上記ログ情報に基づいて上記コンテンツサーバが送信する整合検証値データを受信し、上記制御手段は、上記再生手段がコンテンツデータを再生するときは上記整合検証値データに基づいてコンテンツIDの検証を行うよう制御することを特徴とする請求項7記載のデータ処理装置。

【請求項12】 ネットワークを介してデータ処理装置と接続されたコンテンツサーバであって、

コンテンツデータを記憶する記憶手段と、

上記記憶手段に記憶されたコンテンツデータを上記データ処理装置へ送信する通信手段と、

上記データ処理装置から受信したコンテンツデータのコンテンツIDリストを含むログ情報を上記データ処理装置に対応付けて上記記憶手段に記憶し、上記データ処理装置から要求があった場合、上記通信手段が上記ログ情報に基づいてデータを上記データ処理装置へ送信するよう制御する制御手段と

を有するコンテンツサーバ。

【請求項13】 上記コンテンツIDリストに基づいて送信するデータはコンテンツデータであり、上記制御手段は上記記憶手段に記憶されたコンテンツデータを上記通信手段が送信するよう制御することを特徴とする請求項12記載のコンテンツサーバ。

【請求項14】 上記コンテンツIDリストに基づいて送信するデータは、コンテンツを復号化するためのコンテンツ鍵であることを特徴とする請求項12記載のコンテンツサーバ。

【請求項15】 上記コンテンツIDリストに基づいて整合検証値データを生成する生成手段を有し、

上記制御手段は上記生成手段で生成した整合検証値データを上記データ処理装置へ送信するよう前記通信手段を制御することを特徴とする請求項12記載のコンテンツサーバ。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】 0001

【補正方法】 変更

【補正の内容】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを介して音楽データ等のコンテンツデータを提供するコンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コンテンツサーバに関するものである。

【手続補正4】

【補正対象書類名】 明細書

【補正対象項目名】 0006

【補正方法】 変更

【補正の内容】

【0006】

本発明は、このような実情を鑑みてなされたものであり、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができるコンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コンテンツサーバを提供することを目的とする。

【手続補正5】

【補正対象書類名】 明細書

【補正対象項目名】 0018

【補正方法】 変更

【補正の内容】

【0018】

この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行わせる。

本発明にかかるデータ処理装置は、コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、上記コンテンツサーバとの間でデータを送受信する通信手段と、コンテンツデータを記憶する記憶手段と、上記記憶手段に記憶されたコンテンツデータを再生する再生手段と、上記記憶手段に記憶されたコンテンツデータのコンテンツIDリストを含むログ情報を管理し、上記コンテンツサーバへ上記ログ情報を上記通信手段が送信するよう制御し、上記再生手段が上記コンテンツデータを再生するよう制御する制御手段とを有し、上記記憶手段に記憶された上記コンテンツデータが上記再生手段で再生できなくなったときは、上記通信手段が上記ログ情報に基づいて上記コンテンツサーバが送信するデータを受信することを特徴とする。

このデータ処理装置は、ログ情報に基づいてコンテンツサーバから再配信されたコンテンツデータを受信する。

本発明にかかるコンテンツサーバは、ネットワークを介してデータ処理装置と接続されたコンテンツサーバであって、コンテンツデータを記憶する記憶手段と、上記記憶手段に記憶されたコンテンツデータを上記データ処理装置へ送信する通信手段と、上記データ処理装置から受信したコンテンツデータのコンテンツIDリストを含むログ情報を上記データ処理装置に対応付けて上記記憶手段に記憶し、上記データ処理装置から要求があった場合、上記通信手段が上記ログ情報に基づいてデータを上記データ処理装置へ送信するよう制御する制御手段とを有することを特徴とする。

このコンテンツサーバは、データ処理装置から受信したログ情報をデータ処理装置に対応付けて記憶し、このログ情報に基づいてデータ処理装置にデータを送信する。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-195509

(43)Date of publication of application : 19.07.2001

(51)Int.Cl. G06F 17/60

G10K 15/02

(21)Application number : 2000-326125 (71)Applicant : SONY CORP

(22)Date of filing : 25.10.2000 (72)Inventor : ISHIGURO RYUJI

KAWAKAMI TATSU

TANABE MITSURU

EOMO YUICHI

SATO ICHIRO

EBIHARA SHUGI

(30)Priority

Priority number : 11303138

Priority date : 25.10.1999

Priority country : JP

(54) CONTENTS PROVIDING SYSTEM, CONTENTS DISTRIBUTING METHOD, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To restore contents data while protecting a copyright even when the contents data distributed through a network are temporarily destroyed.

SOLUTION: A PC stores the backup of distributed music contents on a hard disk and transmits the use log information on the music contents stored on the hard disk to an EMD server. When the music contents on the hard disk are destroyed, for example, the PC acquires the use log information from the EMD server and reproduces the backup data stored on the hard disk corresponding to the use log information.

LEGAL STATUS [Date of request for examination] 28.03.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage The contents offer system characterized by carrying out the playback and/or control of backup data of contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and have been memorized to the above-mentioned storage according to this use log information.

[Claim 2] The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution from the above-mentioned contents server, this contents data it became impossible to acquire The contents offer system characterized by carrying out playback and/or control of the contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and were re-distributed according to this use log information.

[Claim 3] The data processor which has the playback control program which carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network While the above-mentioned contents server distributes contents data to the above-mentioned data processor, memorizing to a storage the contents data with which the above-mentioned data processor was distributed from the above-mentioned contents server and carrying out playback and/or control The backup data of the distributed contents data are memorized to a storage. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage The contents distribution approach that the above-mentioned contents server transmits the above-mentioned use log information to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to the above-mentioned use log information.

[Claim 4] The data processor which has the playback control program which carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network The above-mentioned contents server distributes contents data to the above-mentioned data processor. The above-mentioned

data processor memorizes to a storage the contents data distributed from the above-mentioned contents server, and carries out playback and/or control. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage While re-distributing this contents data it became impossible to acquire to the above-mentioned data processor, the above-mentioned contents server The contents distribution approach that the above-mentioned use log information is transmitted to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out playback and/or control of the contents data re-distributed according to the above-mentioned use log information.

[Claim 5] It is installed in a data processor and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage The storage characterized by carrying out the playback and/or control of backup data of contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and have been memorized to the above-mentioned storage according to this use log information.

[Claim 6] It is installed in a data processor and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution from the above-mentioned contents server, this contents data it became impossible to acquire The storage characterized by carrying out playback and/or control of the contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and were re-distributed according to this use log information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the contents offer system and the contents distribution approach of offering contents data, such as music data, through a network, and a storage.

[0002]

[Description of the Prior Art] In recent years, online distribution of the music content using networks, such as the Internet and cable television, began to be put in practical use.

[0003] In the distribution system of such a music content, a contents distribution contractor offers a music content on Web, when distributing a music content through a network. Moreover, the user using this music distribution system accesses Web which a contents distribution contractor offers using a self personal computer, and downloads a desired music content.

[0004]

[Problem(s) to be Solved by the Invention] By the way, generally in such a music distribution system, accounting is carried out through a network as opposed to the downloaded music content.

[0005] However, if the data in the personal computer which a user holds break for example, the once purchased music content will also disappear. Therefore, in order to have restored the music content, contents had to be purchased again.

[0006] This invention is made in view of such the actual condition, and it aims at offering the contents offer system which can restore contents data, the contents distribution approach, and a storage, aiming at protection of copyright, even if the contents data which carried out contents distribution through the network are the case where it has once been destroyed.

[0007]

[Means for Solving the Problem] The contents server to which the contents offer system concerning this invention distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage The above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to this use log information.

[0008] In a contents offer system, a data processor performs playback and/or control of restoration data of backup based on the use log information re-acquired from the contents server.

[0009] In the contents offer system concerning this invention The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution for this contents data it became impossible to acquire from the above-mentioned contents server, the above-

mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out playback and/or control of the contents data re-distributed according to this use log information.

[0010] In this contents offer system, playback and/or control of the contents data with which the data processor was re-distributed based on the use log information re-acquired from the contents server are performed.

[0011] The data processor which has the playback control program with which the contents distribution approach concerning this invention carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network While the above-mentioned contents server distributes contents data to the above-mentioned data processor, memorizing to a storage the contents data with which the above-mentioned data processor was distributed from the above-mentioned contents server and carrying out playback and/or control The backup data of the distributed contents data are memorized to a storage. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage The above-mentioned contents server transmits the above-mentioned use log information to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to the above-mentioned use log information.

[0012] By this contents distribution approach, a data processor performs playback and/or control of restoration data of backup based on the use log information re-acquired from the contents server.

[0013] The data processor which has the playback control program with which the contents distribution approach concerning this invention carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network The above-mentioned contents server distributes contents data to the above-mentioned data processor. The above-mentioned data processor memorizes to a storage the contents data distributed from the above-mentioned contents server, and carries out playback and/or control. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage While re-distributing this contents data it became impossible to acquire to the above-mentioned data processor, the above-mentioned contents server The above-mentioned use log information is transmitted to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out playback and/or control of the contents data re-distributed according to the above-mentioned use log information.

[0014] By this contents distribution approach, playback and/or control of the contents data with which the data processor was re-distributed based on the use log information re-acquired from the contents server are performed.

[0015] The storage concerning this invention is installed in a data processor, and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage The above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to this use log information.

[0016] Playback and/or control of restoration data of backup are made to perform in this storage to the data processor with which the playback control program was installed based on the use log information re-acquired from the contents server.

[0017] The storage concerning this invention is installed in a data processor, and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution for this contents data it became impossible to acquire from the above-mentioned contents server, the above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out playback and/or control of the contents data re-distributed according to this use log information.

[0018] Playback and/or control of the re-distributed contents data are made to perform in this storage to the data processor with which the playback control program was installed based on the use log information re-acquired from the contents server.

[0019]

[Embodiment of the Invention] It explains to a detail, referring to a drawing as a gestalt of the best operation of this invention hereafter about the music content distribution system which applied this invention. This music content distribution system is a system which performs management of the music content which downloaded to the personal computer or the portable device and was further downloaded from the server through the network, or the music content read in CD etc.

[0020] (1) The whole music content distribution system block diagram 1 is drawing showing the whole music content distribution system configuration which applied this invention.

[0021] This music content distribution system is equipped with a personal computer 1, the networks 2, such as the Internet and a Local Area Network, the registration server 3, two or more EMD (Electrical Music Distribution) servers 4 (4-1, 4-2, 4-3) that distribute music data (it is hereafter called contents.), and the WWW server 5 (5-1, 5-2), and is

constituted. Moreover, through the USB cable 7 (7-1, 7-2, 7-3), storages, such as memory card, are stored in the interior and the portable device 6 (6-1, 6-2, 6-3) which is the music regenerator machine of the pocket mold which reproduces contents is connected to a personal computer 1.

[0022] A personal computer 1 is connected with the EMD registration server 3, the EMD server 4 (4-1, 4-2, 4-3), and the WWW (World Wide Web) server 5 (5-1, 5-2) through a network 2.

[0023] From the EMD server 4 (4-1, 4-2, 4-3), a personal computer 1 receives the contents compressed by the predetermined compression method, and enciphers and records them with a predetermined cipher system. Moreover, a personal computer 1 compresses the contents read in CD (Compact Disc) etc. by the predetermined compression method, and enciphers and records them with a predetermined cipher system. As a compression method, methods, such as ATRAC (Adaptive Transform Acoustic Coding)³ (trademark) and MP3 (MPEG Audio Layer-3), are used, for example. Moreover, DES (Data Encryption Standard) etc. is used as a cipher system.

[0024] Moreover, when receiving distribution of contents, a personal computer 1 also receives distribution of the use condition information which shows the use conditions of the contents, and records it. Moreover, when recording the contents read in CD etc., according to the playback conditions of the contents, a personal computer 1 generates use condition information, and records it.

[0025] Moreover, a personal computer 1 updates use condition information corresponding to having recorded the contents currently enciphered and recorded on the portable device 6 (6-1, 6-2, 6-3), and having made them memorize with related information, such as use condition information and a music name, and a player, through the USB cable 7 (7-1, 7-2, 7-3). This processing is called check-out. Use condition information carries out 1 **** of the counts of the contents which the personal computer 1 is recording and which can be checked out, when you check out. Corresponding contents cannot be checked out when the count which can be checked out is 0.

[0026] Moreover, a personal computer 1 is made to respond to having eliminated and (or not using it and putting) eliminated the contents memorized by the portable device 6 (6-1, 6-2, 6-3) through the USB cable 7 (7-1, 7-2, 7-3), and updates use condition information. This elimination processing is called check-in. When you check in, 1 **** of the counts of the contents which the personal computer 1 is recording and which can be checked out is carried out.

[0027] In addition, to the contents which other personal computers checked out to the portable device 6, check-in cannot do a personal computer 1. That is, he can check in only at the contents which personal computer 1 self checked out.

[0028] When, as for the EMD registration server 3, a personal computer 1 starts acquisition of contents from the EMD server 4 (4-1, 4-2, 4-3), A network 2 is minded corresponding to the demand of a personal computer 1. While transmitting an authentication key required for the mutual recognition of a personal computer 1 and the EMD server 4 (4-1, 4-2, 4-3) to a personal computer 1 The program for connecting with the EMD server 4 (4-1, 4-2, 4-3) is transmitted to a personal computer 1.

[0029] The EMD server 4 (4-1, 4-2, 4-3) supplies contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1 with the

associated data (for example, a music name or a player etc.) of use condition information and contents.

[0030] The contents which each EMD server 4 (4-1, 4-2, 4-3) distributes are compressed by the method of predetermined compression. The compression methods may differ for every server. Moreover, the contents which each EMD server 4 (4-1, 4-2, 4-3) supplies are enciphered and distributed with a predetermined cipher system. The cipher systems may differ for every server.

[0031] The WWW server 5 (5-1, 5-2) supplies the data (for example, a music name or a composer name etc.) corresponding to the contents read in CDs (for example, the album name of CD or the selling firm of CD etc.) and CD which read contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1.

[0032] The portable device 6 (6-1, 6-2, 6-3) is equipment which is reproduced and outputs the contents (namely, checked-out contents) supplied from the personal computer 1 to the headphone which are not illustrated.

[0033] Each portable device 6 (6-1, 6-2, 6-3) has the storage for memorizing contents. As a storage, the IC memory in which removal with which the internal substrate of equipment was equipped is impossible, the memory card which can be detached and attached are used, for example. The portable device 6 (6-1, 6-2, 6-3) is connected with a personal computer 1 through the physical interfaces 7 (7-1, 7-2, 7-3), such as USB, and contents are transmitted. At this time, contents are transmitted in the condition of having been enciphered and compressed, and use condition information is also added.

[0034] Each portable device 6 (6-1, 6-2, 6-3) will be reproduced by reading the enciphered contents from a storage, if it is usually used where connection with a personal computer 1 is separated, and a playback instruction is given by the user in this condition. Moreover, based on the use condition information added to each contents, restrict playback, deletion of contents etc. is controlled, or each portable device 6 (6-1, 6-2, 6-3) performs renewal of use condition information etc. if needed.

[0035] Hereafter, when it is not necessary to distinguish the portable device 6-1, 6-2, and 6-3 separately, the portable device 6 is only called.

[0036] Next, the configuration of a personal computer 1 is explained with reference to drawing 2.

[0037] CPU (Central Processing Unit)11 actually performs various application programs (for details, it mentions later.) and OS (Operating System). Generally ROM (Read-only Memory)12 stores the data of immobilization fundamentally of the parameters the program which CPU11 uses, and for an operation. RAM (Random Access Memory)13 stores a variable parameter suitably in the program used in activation of CPU11, and its activation. These are mutually connected by the host bus 14 which consists of CPU buses etc.

[0038] The host bus 14 minds a bridge 15 and is PCI (Peripheral ComponentInterconnect/Interface). It connects with the external buses 16, such as a bus.

[0039] A keyboard 18 is operated by the user when inputting various kinds of commands into CPU11. A mouse 19 is operated by the user when performing the directions and selection of the point on the screen of a display 20. A display 20 consists of a liquid crystal display or CRT (Cathode Ray Tube), and displays various information

in a text or an image. HDD (Hard Disk Drive) 21 drive a hard disk, and record or reproduce the program and information which are performed by CPU11 to them.

[0040] Drive 22 reads the data or the program currently recorded on the magnetic disk 41 with which it is equipped, an optical disk 42 (CD is included), a magneto-optic disk 43, or semiconductor memory 44, and supplies the data or program to RAM13 with which it connects through the interface 17, the external bus 16, the bridge 15, and the host bus 14.

[0041] The portable device 6 (6-1, 6-2, 6-3) is connected to the USB port 23 (23-1, 23-2, 23-3) through the USB cable 7 (7-1, 7-2, 7-3). The USB port 23 outputs the data (for example, the command of contents or the portable device 6 etc. is included) supplied from HDD21, CPU11, or RAM13 through an interface 17, an external bus 16, a bridge 15, or the host bus 14 to the portable device 6 (6-1, 6-2, 6-3).

[0042] The voice-input/output interface 24 which has IEC(International Electrotechnical Commission) 60958 terminal 24a performs interface processing of digitized voice I/O or an analog voice input/output. A loudspeaker 45 outputs the predetermined voice corresponding to contents based on the sound signal supplied from the voice-input/output interface 24.

[0043] These keyboards 18, a mouse 19, a display 20, HDD21, the drive 22, the USB port 23, and the voice-input/output interface 24 are connected to the interface 17, and the interface 17 is connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.

[0044] A network 2 is connected and the communications department 25 stores in the packet of a predetermined method the data (for example, the demand of registration or the Request to Send of contents etc.) supplied from CPU11 or HDD21. While transmitting through a network 2, the data (for example, an authentication key or contents etc.) stored in the packet which received are outputted to CPU11, RAM13, or HDD21 through a network 2.

[0045] Formed in one as a semiconductor IC, CPU32 of the adapter 26 with which a personal computer 1 is equipped has two incomes with CPU11 of a personal computer 1 through an external bus 16, a bridge 15, and the host bus 14, and performs various kinds of processings. CPU32 performs various kinds of processings upwards, and RAM33 memorizes required data and a required program. Nonvolatile memory 34 memorizes the data which need to be held even after the power source of a personal computer 1 is turned off. When the program enciphered has been transmitted to ROM36 from the personal computer 1, the program which decodes it is memorized. RTC (Real Time Clock)35 -- a time check -- actuation is performed and time information is offered. The semiconductor IC is designed by the secure environment and has resistance to access malicious from the outside. In addition, this function may consist of software programs.

[0046] The communications department 25 and an adapter 26 are connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.

[0047] Next, the configuration of the portable device 6 is explained with reference to drawing 3.

[0048] A power circuit 52 makes the portable device 6 whole drive by transforming into the internal power of a predetermined electrical potential difference the supply voltage supplied from a dry cell 51, and supplying CPU53 - a display 67.

[0049] The USB controller 57 supplies the data containing the contents transmitted from the personal computer 1 to CPU53 through an internal bus 58, when it connects with a personal computer 1 through the USB cable 7 through the USB connector 56.

[0050] The data transmitted from a personal computer 1 consist of 64 bytes per one packet of data, and are transmitted from a personal computer 1 at the transfer rate of 12 Mbit/sec.

[0051] The data transmitted to the portable device 6 consist of a header and contents. While content ID, a file name, header size, a contents key, a file size, Codec ID, file information, etc. are stored, use condition information required for playback limit processing etc. is stored in the header. Contents are encoded and enciphered by coding methods, such as ATRAC3.

[0052] Header size expresses the data lengths (for example, 33 etc. bytes etc.) of a header, and a file size expresses the data lengths (for example, 33,636,138 etc. bytes etc.) of contents.

[0053] A contents key is a key for decoding the contents enciphered, and is transmitted to the portable device 6 from a personal computer 1 in the condition of having been enciphered based on the session key (momentary key) generated by processing of the mutual recognition of a personal computer 1 and the portable device 6.

[0054] When the portable device 6 is connected to the USB port 23 of a personal computer 1 through the USB cable 7, the portable device 6 and a personal computer 1 perform processing of mutual recognition. Processing of this mutual recognition is processing of authentication of for example, a challenge response method. Incidentally, DSP59 of the portable device 6 performs processing of decryption (decode), when processing authentication of a challenge response method.

[0055] A challenge response method is a method which answers with the value (response) which the portable device 6 generated to a certain value (challenge) which a personal computer 1 generates using the private key currently shared with a personal computer 1. Since the value which a personal computer 1 generates changes for every processing of authentication in processing of the mutual recognition of a challenge response method each time, even if the value which the portable device 6 outputted and which was generated using the private key is read for example, and it receives the so-called attack of spoofing, since the values used for mutual recognition differ, by processing of the following mutual recognition, as for a personal computer 1, injustice is detectable.

[0056] Content ID is ID for specifying contents corresponding to contents.

[0057] Codec ID is ID corresponding to the coding method of contents, for example, codec ID"1" corresponds to ATRAC3, and codec ID"0" corresponds to MP3 (MPEG (Moving Picture Experts Group) Audio Layer-3).

[0058] A file name is ASCII (American National Standard Code for Information Interchange) about the contents file (it mentions later) which the personal computer 1 corresponding to contents is recording. It is data converted with the code and file information is data which changed the music name corresponding to contents, the artist name, the songwriter name, or the composer name into the ASCII code.

[0059] When the portable device 6 receives the write-in instruction of contents with contents from a personal computer 1, CPU53 which performs the main program read from RAM54 or ROM55 makes the contents which controlled reception and the flash

memory controller 60 and received the write-in instruction from the personal computer 1 write in a flash memory 61.

[0060] A flash memory 61 has the storage capacity of about 64 MByte(s), and memorizes contents. Moreover, the code for playback for elongating the contents compressed by the predetermined compression method is beforehand stored in the flash memory 61.

[0061] In addition, you may enable it to make a flash memory 61 removable as a memory card at the portable device 6.

[0062] When the playback instruction corresponding to depression actuation of the playback/earth switch which is not illustrated by the user is supplied to CPU53 through the actuation key controller 62, CPU53 makes the flash memory controller 60 read the code for playback, and contents, and DSP59 is made to transmit it to it from a flash memory 61.

[0063] DSP59 is based on the code for playback transmitted from the flash memory 61, and is CRC (Cyclic Redundancy Check) about contents. After carrying out error detection by the method, it reproduces and the reproduced data (D1 shows in drawing 3) are supplied to the digital to analog circuit 63.

[0064] DSP59 supplies the clock LRCLK of operation which becomes the predetermined bit clock BCLK and the predetermined list of a frequency which were generated based on the master clock MCLK and the master clock MCLK in the internal oscillator circuit from the L channel clock LCLK of a frame unit, and the R channel clock RCLK to the digital-to-analog conversion circuit 63 while reproducing contents based on the master clock MCLK from dispatch child 59A which changes with Xtal by which was constituted by one and external was carried out to it with the dispatch circuit established in the interior.

[0065] When supplying an above-mentioned clock of operation to the digital-to-analog conversion circuit 63 according to the code for playback when reproducing contents, and not reproducing contents, DSP59 suspends supply of a clock of operation according to the code for playback, stops the digital-to-analog conversion circuit 63, and reduces the consumed electric power of the portable device 6 whole.

[0066] Similarly, external [of radiator 53A or 57A which CPU53 and the USB controller 57 also become with Xtal] is carried out, respectively, and it performs predetermined processing based on the master clock MCLK supplied from radiator 53A or 57A, respectively.

[0067] Thus, with constituting, the clock generation module for performing clock supply to each circuit block of CPU53, DSP59, and USB controller 57 grade becomes unnecessary, and the portable device 6 can be miniaturized while simplifying circuitry.

[0068] The digital-to-analog conversion circuit 63 changes the reproduced contents into the sound signal of an analog, and supplies this to an amplifying circuit 64. An amplifying circuit 64 amplifies a sound signal and supplies a sound signal to headphone through the headphone jack 65.

[0069] Thus, the portable device 6 suspends playback of contents, when press actuation of playback/the earth switch is carried out during playback, while reproducing the contents memorized by the flash memory 61 based on control of CPU53, when press actuation of playback/the earth switch is carried out.

[0070] The portable device 6 resumes playback of contents from the location stopped based on control of CPU53, when press actuation of playback/the earth switch is again carried out after a halt. When it passes for several seconds, without playback/earth switch suspending playback by press actuation, and adding actuation, the portable device 6 turns off a power source automatically, and reduces power consumption.

[0071] Incidentally, when press actuation of playback/the earth switch is carried out after the power source became off, the portable device 6 does not reproduce contents from the location which last time stopped, but reproduces them from the 1st music.

[0072] moreover, CPU53 of the portable device 6 -- the LCD controller 68 -- controlling - a display 67 -- the condition of a playback mode, equalizer adjustments (for example, repeat playback, intro playback, etc.) (namely, adjustment of the gain corresponding to the frequency band of a sound signal), a tune number number, performance time amount, playback, a halt, and a rapid traverse -- information, such as conditions, such as return, sound volume, and a residue of a dry cell 51, is already displayed.

[0073] Furthermore, the portable device 6 stores the so-called FAT (File Allocation Table), such as a block location of a flash memory 61 where the number of the contents currently written in the flash memory 80 and each contents are written in EEPROM68, and various memory are recording information in addition to this.

[0074] Incidentally, in the gestalt of this operation, contents are treated considering 64KByte as 1 block, and the block location corresponding to the contents of one music is stored in FAT.

[0075] If the block location corresponding to the contents of the 1st music will be written in a flash memory 61 as FAT if the contents of the 1st music are written in a flash memory 61 by control of CPU53, next the contents of the 2nd music are written in a flash memory 61 when FAT is stored in a flash memory 61 for example, the block location corresponding to the contents of the 2nd music will be written in a flash memory 61 (the same field as the 1st music) as FAT.

[0076] Thus, FAT is rewritten at every writing of the contents to a flash memory 61, and the same data are further written in reserve at a duplex for protection of data.

[0077] If FAT is written in a flash memory 61, since the same field of a flash memory 61 will be rewritten twice corresponding to one writing of contents, by the count of little writing of contents, the count of rewriting specified to the flash memory 61 will be become, and rewriting of a flash memory 61 will become impossible.

[0078] Then, the portable device 6 makes EEPROM68 memorize FAT, and lessens the frequency of rewriting of the flash memory 61 corresponding to one writing of contents.

[0079] By making EEPROM68 memorize FAT with many counts of rewriting, the portable device 6 can increase the count which can do the writing of contents to dozens or more times as compared with the case where a flash memory 61 is made to memorize FAT. Furthermore, since CPU53 is made to write in so that FAT may be added to EEPROM68, it prevents lessening the frequency of rewriting of the same field of EEPROM68, and EEPROM68 rewriting for a short period of time, and becoming impossible.

[0080] The portable device 6 recognizes that USB connection was made based on the interrupt signal supplied to CPU53 from the USB controller 57, when it connects with a personal computer 1 through the USB cable 7 (this is hereafter called USB connection).

[0081] The portable device 6 controls a power circuit 52, and stops supply of the power from a dry cell 51 while it will receive supply of the external power of a convention current value from a personal computer 1 through the USB cable 7, if it recognizes that USB connection was made.

[0082] CPU53 stops processing of playback of the contents of DSP59, when USB connection is made. Thereby, CPU53 prevents that the external power supplied from a personal computer 1 exceeds a convention current value, and controls it to be always able to receive the external power of a convention current value.

[0083] Thus, if USB connection is made, since CPU53 will be switched to the power supplied from a personal computer 1 from the power supplied from a dry cell 51, the external power from the personal computer 1 with a cheap power unit price is used, the power consumption of the dry cell 51 with a high power unit price is reduced, and it can prolong the life of a dry cell 51 in this way.

[0084] In addition, when supply of external power is received from a personal computer 1 through the USB cable 7, by stopping regeneration of DSP59, CPU53 reduces the radiation from DSP59, and reduces much more radiation of the whole system which contains a personal computer 1 as the result.

[0085] The function of the personal computer 1 realized next by the program execution installed in the personal computer 1 is explained.

[0086] Drawing 4 is drawing which is realized by predetermined program execution etc. and in which showing the configuration of the function of a personal computer 1.

[0087] The contents manager 111 consists of two or more programs, such as the EMD selection program 131, check-in/check-out manager 132, the copy manager 133, the migration manager 134, the cipher system conversion program 135, the compression method conversion program 136, the encryption program 137, the use condition conversion program 139, the use condition manager 140, the authentication program 141, the decode program 142, the driver 143 for PD, the program 144 for purchase, and the program 145 for purchase.

[0088] the contents manager 111 -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the contents manager 111 directly) -- it is constituted like.

[0089] When the contents manager 111 is installed in a personal computer 1, the EMD selection program 131 is not included in the contents manager 111, but is received from the EMD registration server 3 through a network 2 in the case of registration of EMD. The EMD selection program 131 chooses connection with that [EMD server 4 (4-1, 4-2, 4-3)], and makes the application 115 for purchase, or the program 144,145 for purchase perform the communication links (for example, download of contents when purchasing contents etc.) with the EMD server 4 (4-1, 4-2, 4-3).

[0090] Check-in/check-out manager 132 checks in at the contents which check out the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on check-in or a setup of check-out and the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or are memorized by the portable device 6.

[0091] Check-in/check-out manager 132 updates the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N corresponding to processing of check-in or check-out.

[0092] The copy manager 133 copies the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or copies contents to the contents database 114 from the portable device 6.

[0093] The migration manager 134 moves the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or moves contents to the contents database 114 from the portable device 6.

[0094] The cipher system conversion program 135 is changed into the method of the same encryption as the contents stored in the contents file 161-1 on which the contents database 114 is recording the method of encryption of the contents which the application program 115 for purchase received from the EMD server 4-1, and the method of encryption of the contents which the program 144 for purchase received from the EMD server 4-2 - 161-N through a network 2.

[0095] The compression method conversion program 136 is changed into the method of the same compression as the contents stored in the contents file 161-1 on which the contents database 114 is recording the method of compression of the contents which the application program 115 for purchase received from the EMD server 4-1, and the method of compression of the contents which the program 144 for purchase received from the EMD server 4-2 - 161-N through a network 2.

[0096] It is read in CD and the encryption program 137 is enciphered by the method of the same encryption as the contents stored in the contents file 161-1 on which the contents database 114 is recording the contents (not enciphered) supplied from the sound recording program 113 - 161-N.

[0097] It is read in CD and compression/elongation program 138 is encoded by the method of the same coding as the contents stored in the contents file 161-1 on which the contents database 114 is recording the contents (not compressed) supplied from the sound recording program 113 - 161-N. Compression/elongation program 138 elongates the contents encoded (decode).

[0098] The use condition conversion program 139 is changed into the same format as the use condition information stored in the use condition file 162-1 on which the contents database 114 is recording the use condition information on the contents which the application program 115 for purchase received from the EMD server 4-1 (the so-called Usage Rule), and the use condition information on the contents which the program 144 for purchase received from the EMD server 4-2 - 162-N through a network 2.

[0099] The use condition manager 140 detects the alteration of use condition information based on the hash value corresponding to the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N, before performing processing of the copy of contents, migration, check-in, or check-out. The use condition manager 140 updates the hash value corresponding to use condition information for the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N accompanying

processing of the copy of contents, migration, check-in, or check-out corresponding to updating.

[0100] The authentication program 141 performs processing of the mutual recognition of the contents manager 111 and the application program 115 for purchase, and processing of the mutual recognition of the contents manager 111 and the program 144 for purchase. Moreover, the authentication program 141 has memorized the authentication key used by processing of the mutual recognition of the EMD server 4-3 and the program 145 for purchase.

[0101] The authentication key which the authentication program 141 uses by processing of mutual recognition is not memorized by the authentication program 141 when the contents manager 111 is installed in a personal computer 1, but when processing of registration is normally performed by the display operator guidance program 112, is supplied from the EMD registration server 3, and is memorized by the authentication program 141.

[0102] The decode program 142 decodes contents, when a personal computer 1 reproduces the contents stored in the contents file 161-1 which the contents database 114 is recording - 161-N.

[0103] The driver 143 for PD supplies the command which makes the portable device 6 perform predetermined processing to contents or the portable device 6, when you check out predetermined contents to the portable device 6, or when you check in at predetermined contents from a portable device.

[0104] The program 144 for purchase is installed with the contents manager 111, is supplied through a network 2 from the EMD registration server 3, or is recorded on predetermined CD and supplied. The program 144 for purchase transmits and receives the contents manager 111 and data through the interface of the predetermined format which the contents manager 111 has, when installed in a personal computer 1.

[0105] the program 144 for purchase -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the program 144 for purchase directly) -- it is constituted like.

[0106] The program 144 for purchase receives contents from the EMD server 4-2 while requiring transmission of predetermined contents of the EMD server 4-2 through a network 2. Moreover, the program 144 for purchase performs processing of accounting, when receiving contents from the EMD server 4-2.

[0107] The program 145 for purchase is a program installed with the contents manager 111, and it receives contents from the EMD server 4-3 while it requires transmission of predetermined contents of the EMD server 4-3 through a network 2. Moreover, the program 145 for purchase performs processing of accounting, when receiving contents from the EMD server 4-3.

[0108] The display operator guidance program 112 displays the image of a predetermined window on a display 20 based on the filtering data file 181, the display data file 182, an image file 183-1 - 183-K, or the hysteresis data file 184, and directs activation of processings, such as check-in or check-out, based on the actuation to a keyboard 18 or a mouse 19 at the contents manager 111.

[0109] The filtering data file 181 stores the data for making weighting each contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N, and is recorded on HDD21.

[0110] The display data file 182 stores the data corresponding to the contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N, and is recorded on HDD21.

[0111] An image file 183-1 - 183-K store the image corresponding to the contents file 161-1 currently recorded on the contents database 114 - 161-N, or the image corresponding to the package mentioned later, and are recorded on HDD21.

[0112] Hereafter, when it is not necessary to distinguish an image file 183-1 - 183-K separately, an image file 183 is only called.

[0113] The contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N store historical data, such as a checked-out count, a count at which he checked in, and its date, and the hysteresis data file 184 is recorded on HDD21.

[0114] The display operator guidance program 112 receives the key for authentication, and the EMD selection program 131 from the EMD registration server 3, and supplies the key for authentication, and the EMD selection program 131 to the contents manager 111 while it transmits ID of the contents manager 111 beforehand memorized to the EMD registration server 3 through a network 2 at the time of processing of registration.

[0115] The sound recording program 113 displays the image of a predetermined window, and reads data, such as sound recording time amount of contents, from CD which is the optical disk 42 with which the drive 22 was equipped based on the actuation to a keyboard 18 or a mouse 19.

[0116] The sound recording program 113 minds a network 2 based on the sound recording time amount of the contents currently recorded on CD etc. While requiring transmission of the data (for example, music name etc.) corresponding to the contents currently recorded on the WWW server 5-1 or 5-2 by the data (for example, an album name or an artist name etc.) or CD corresponding to CD The data corresponding to the contents currently recorded on the data or CD corresponding to CD from the WWW server 5-1 or 5-2 are received.

[0117] The sound recording program 113 supplies the data corresponding to the contents currently recorded on the data or CD corresponding to received CD to the display operator guidance program 112.

[0118] Moreover, when directions of sound recording are inputted, the sound recording program 113 reads contents from CD which is the optical disk 42 with which the drive 22 was equipped, and outputs them to the contents manager 111.

[0119] The contents which the contents database 114 is compressed by the predetermined method supplied from the contents manager 111, and are enciphered by the predetermined method are stored in either the contents file 161-1 - 161-N (it records on HDD21). The contents database 114 is stored in either the use condition file 162-1 corresponding to the contents file 161-1 by which the use condition information corresponding to the contents stored in the contents file 161-1 - 161-N, respectively is stored in contents - 161-N - 162-N, respectively (it records on HDD21).

[0120] The contents database 114 may record the contents file 161-1 - 161-N, or the use condition file 162-1 - 162-N as a record.

[0121] For example, the use condition information corresponding to the contents stored in the contents file 161-1 is stored in the use condition file 162-1. The use condition information corresponding to the contents stored in contents file 161-N is stored in use condition file 162-N.

[0122] Hereafter, when it is not necessary to distinguish the contents file 161-1 - 161-N separately, the contents file 161 is only called. Hereafter, when it is not necessary to distinguish the use condition file 162-1 - 162-N separately, the use condition file 162 is only called.

[0123] The application program 115 for purchase is supplied through a network 2 from the EMD registration server 3, or is recorded and supplied to predetermined CD-ROM. The application program 115 for purchase receives contents from the EMD server 4-1, and supplies them to the contents manager 111 while it requires transmission of predetermined contents of the EMD server 4-1 through a network 2. Moreover, the application program 115 for purchase performs processing of accounting, when receiving contents from the EMD server 4-1.

[0124] Next, matching with the data stored in the display data file 182, and the contents file 161-1 stored in the contents database - 161-N is explained.

[0125] The contents stored in either the contents file 161-1 - 161-N belong to a predetermined package. A package is either an original package and my selection package or a filtering package more at a detail.

[0126] One or more contents belong and an original package is equivalent to the classification (for example, it corresponds to the so-called album) of the contents in the EMD server 4, or CD of one sheet. Contents cannot belong to one of original packages, and cannot belong to two or more original packages. Moreover, the original package with which contents belong cannot be changed. A user can edit a part of information corresponding to an original package (modification of the information which information added or added).

[0127] One or more contents from which the user chose the my selection package as arbitration belong. A user can edit into arbitration whether which contents belong to a my selection package. Contents can belong to one or more my selection packages at coincidence. Moreover, contents do not need to belong to which my selection package.

[0128] The contents chosen based on the filtering data stored in the filtering data file 181 belong to a filtering package. Filtering data are supplied through a network 2 from the EMD server 4 or the WWW server 5, or are recorded on predetermined CD and supplied. A user can edit the filtering data stored in the filtering data file 181.

[0129] Filtering data serve as criteria which choose predetermined contents or compute the weight corresponding to contents. For example, if the filtering data corresponding to the J-POP (pop of Japan) top ten of this week are used, a personal computer 1 can specify the contents of the 10th place of the pop of Japan of the contents of the 1st place of the pop of Japan of this week - this week.

[0130] The filtering data file 181 contains the filtering data with which the period checked out in January [past] chooses contents as long order, the filtering data which choose contents with many counts checked out at past half a year, or the filtering data which chooses the contents by which the alphabetic character of "love" is contained in the music name.

[0131] Thus, the contents of a filtering package make the indicative data 221 (the data which the user set as the indicative data 221 for contents are included) for contents corresponding to contents or historical data 184, and filtering data correspond, and are chosen.

[0132] A driver 117 outputs the analog signal corresponding to the contents which drove the voice-input/output interface 24 on the radical of control, such as the contents manager 111, and outputted to it the contents which inputted the contents which are digital data supplied from the outside, and supplied the contents manager 111, or were supplied from the contents database 114 through the contents manager 111 as digital data, or were supplied to it from the contents database 114 through the contents manager 111.

[0133] Drawing 5 is drawing showing the example of the display operator guidance window which the operator guidance program 112 displays on a display 20, when starting the display operator guidance program 112.

[0134] In order to edit the carbon button 203 for displaying the field which sets up processing of the carbon button 202 for making a display operator guidance window start the carbon button 201 for starting the sound recording program 113, and the EMD selection program 131, check-in, or check-out, and a my selection package, the carbon button 204 grade for displaying the field is arranged.

[0135] When the carbon button 205 is chosen, the data corresponding to an original package are displayed on the field 211. When the carbon button 206 is chosen, the data corresponding to a my selection package are displayed on the field 211. When the carbon button 207 is chosen, the data corresponding to a filtering package are displayed on the field 211.

[0136] The data displayed on the field 211 are data about a package, for example, are a package name or an artist name.

[0137] for example, -- drawing 5 -- setting -- a package -- a name -- " -- the first -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- a package -- a name -- " -- second -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- etc. -- the field -- 211 -- displaying -- having .

[0138] The data corresponding to the contents belonging to the package chosen in the field 211 are displayed on the field 212. The data displayed on the field 212 are for example, a music name, performance time amount, or the count that can be checked out.

[0139] For example, in drawing 5 , since the package corresponding to package name "second" is chosen Bar" and the count which can be checked out of package name "music name corresponding to contents belonging to package corresponding to second"" south (for example, one of the eighth notes is equivalent to one check-out, and an eighth note shows two check-out by two), and a list -- a music name -- "a north graveyard", the count (an eighth note shows one check-out by one) which can be checked out are displayed on the field 212.

[0140] Thus, it is shown that corresponding contents can check out once one eighth note as a count which is displayed on the field 212 and which can be checked out.

[0141] The rest as a count which is displayed on the field 212 and which can be checked out cannot check out corresponding contents (the count which can be checked out is 0.). (-- however, a personal computer 1 can reproduce the contents.) -- things are

shown. Moreover, the G clef as a count which is displayed on the field 212 and which can be checked out shows what no limit is in the count of check-out of corresponding contents (he can check out any number of times).

[0142] In addition, as shown in drawing 5 , it not only displays the count which can be checked out by the number of predetermined graphic forms (for example, a circle, a star, the moon, etc. are sufficient), but you may display it in a figure etc.

[0143] Moreover, the field 208 which displays the image matched with the package or contents chosen on a display operator guidance window (it corresponds to either the image file 183-1 of drawing 4 - 183-K) is arranged. A carbon button 209 is clicked when reproducing the contents chosen (the voice corresponding to contents is made to output to a loudspeaker 45).

[0144] When a carbon button 205 is chosen and the data corresponding to an original package are displayed on the field 211, and choosing the music name of the predetermined contents currently displayed on the field 212 and operating elimination, the display operator guidance program 112 makes the predetermined contents stored in the contents database 114 corresponding to the music name chosen as the contents manager 111 eliminate.

[0145] When the carbon button (carbon button 255 mentioned later) of the window which the sound recording program 113 displays is chosen, it is (activated) and the contents read from CD are recorded on the contents database 114, the display operator guidance program 112 displays the field 213 which displays the music name of the contents memorized by the portable device 6 beforehand specified as the display operator guidance window.

[0146] When the carbon button of the window which the sound recording program 113 displays is chosen and the contents read from CD are recorded on the contents database 114, the display operator guidance program 112 makes the portable device 6 specified beforehand check out the contents which were recorded on the contents database 114 at the contents manager 111 and which were read from CD.

[0147] The music name of contents is made to correspond to the field 213, and the notation which shows whether the contents can check in at a personal computer 1 is displayed on the leftmost of the field 213. For example, "O" located in the leftmost of the field 213 shows what (that is, the personal computer 1 was checked out) the contents corresponding to the music name of contents can check in at a personal computer 1. "x" located in the leftmost of the field 213 shows what (that is, a personal computer 1 is not checked out, for example, other personal computers were checked out) the contents corresponding to the music name of contents cannot check in at a personal computer 1.

[0148] When a display operator-guidance program 112 displays the field 213 on a display operator-guidance window, a display operator-guidance program 112 displays the carbon button 215 which performs the carbon button 210 and the check-in, or the check-out for closing the field 214 and the field 213 which display the name of the portable package (package with which the contents memorized by the portable device 6 belong) with which the contents memorized by the portable device 6 beforehand specified as the display operator-guidance window belong.

[0149] When the display operator guidance program 112 displays the field 213 on a display operator guidance window, furthermore, the display operator guidance program 112 In a display operator guidance window The carbon button 216 which sets up check-

out of the contents corresponding to the music name chosen in the field 212, A setup of the carbon button 217 which sets up check-in of the contents corresponding to the music name chosen in the field 213, the carbon button 218 which sets up check-in of all the contents corresponding to the contents name displayed on the field 213 and check-in, or check-out The carbon button 219 to cancel is arranged.

[0150] Only by setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, a personal computer 1 does not perform processing of check-in or check-out.

[0151] When a carbon button 215 is clicked after carrying out a setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, the display operator guidance program 112 makes the contents manager 111 perform processing of check-in or check-out. When a carbon button 215 is clicked, namely, the display operator guidance program 112 It is based on a setup of check-in or check-out. To the contents manager 111 While making contents transmit to the portable device 6 or making the predetermined commands (for example, command which makes the predetermined contents which the portable device 6 has memorized eliminate) corresponding to check-in transmit The use condition information stored in the use condition file 162 corresponding to the transmitted contents or the command is made to update.

[0152] When check-in or check-out is performed, the display operator guidance program 112 updates the historical data stored in the hysteresis data file 184 corresponding to the contents which transmitted, or the transmitted command. Historical data consist of the name of the information which specifies the contents checked in or checked out or the date checked in or checked out in the contents, and the portable device 6 with which he was checked out in the contents etc.

[0153] Since processing of a setup of check-in or check-out can be performed in a short time, a user can know quickly the condition after check-in or activation of processing of check-out, the count of processing of the check-in which time amount requires, or check-out can be reduced, and the whole (a setup and activation are contained) time amount required for check-in or check-out can be shortened.

[0154] Drawing 6 is drawing explaining the example of the window which the sound recording program 113 displays on a display 20.

[0155] For example, the sound recording program 113 displays the title of CDs, such as "ASHINKURONAIZUDO", on the field 251 based on the information on CD received from the WWW server 5-2. Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays artist names, such as an "arrowhead", on the field 252.

[0156] Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays music names, such as "heat", a "planet", "black", and "Seoul", on the part which displays the music name of the field 253. Similarly, the sound recording program 113 displays artist names, such as an "arrowhead", on the part which displays the artist of the field 253.

[0157] After the sound recording program 113 receives the information on predetermined CD, the sound recording program 113 stores the information on CD in the predetermined directory of HDD21.

[0158] When a carbon button 254 etc. is clicked and directions of acquisition of the information on CD are received, as for the sound recording program 113, the predetermined directory of HDD21 is searched first. The sound recording program 113

makes it choose whether the dialog box which is not illustrated is displayed and the information on CD stored in the user to the directory is used, when the information on CD is stored in the directory.

[0159] When the carbon button 256 which directs initiation of the sound recording of the contents arranged in the window which the sound recording program 113 displays is clicked, the sound recording program 113 supplies the contents which read contents from CD stored in the drive 22, and were read from CD to the contents manager 111 with the information on CD. Compressing compression/elongation program 138 of the contents manager 111 by the method of predetermined compression of the contents supplied from the sound recording program 113, the encryption program 137 enciphers the compressed contents. Moreover, the use condition conversion program 139 is compressed and generates the use condition information corresponding to the enciphered contents.

[0160] The contents manager 111 is compressed and supplies the enciphered contents to the contents database 114 with use condition information.

[0161] The contents database 114 stores use condition information in the use condition file 162 while it generates the contents file 161 and the use condition file 162 corresponding to the contents which received from the contents manager 111 and stores contents in the contents file 161.

[0162] The contents manager 111 supplies the information and use condition information on CD which were received from the sound recording program 113 to the display operator guidance program 112, when the use condition information corresponding to contents and contents is stored in the contents database 114.

[0163] The display operator guidance program 112 generates the data for a display stored in the display data file 182 based on the use condition information corresponding to the contents stored in the contents database 114 by processing of sound recording, and the information on CD.

[0164] In the window which the sound recording program 113 displays, when the contents read from CD are further recorded on the contents database 114, the carbon button 255 which sets up whether the portable device 6 is made to check out the contents read from CD is arranged automatically.

[0165] For example, when a carbon button 255 is clicked, the sound recording program 113 displays the pull down menu which shows the portable device 6. When a user chooses the portable device 6 from the pull down menu, he checks out the contents automatically recorded on the selected portable device 6 from CD. When a user chooses "he not checking out" out from the pull down menu, when contents are recorded from CD, he does not check out a personal computer 1.

[0166] Thus, when the contents read from CD are recorded on the contents database 114 only by activating the carbon button 255 of the window which the sound recording program 113 displays, the contents read from CD to the portable device 6 specified beforehand can be made to check out a personal computer 1.

[0167] (2) the contents distribution contractor who is at the handling during a different format, and the time, and offers a music content -- many -- existing -- every distribution contractor -- the cipher system and compression method of the contents -- formats of use condition information differ further. Therefore, generally the user had to purchase the contents management application and the portable device for playback, or check-

in/check-out for every distribution contractor of contents to receive offer. Therefore, the user was able to deal with the music content stored on one personal computer neither with one management application nor portable device.

[0168] So, in this system, the contents from which a format differs for every distribution contractor in this way are systematically dealt with on the personal computer 1.

[0169] Hereafter, the unified handling of the contents from which a format differs for every distribution contractor in this music content distribution system is explained with reference to drawing 7.

[0170] Two or more EMD servers connected to the network 2 shall be EMD (server A) 4-1 which distributes the music content offered from the music offer firm A, EMD (server B) 4-2 which distribute the music content offered from the music offer firm B, and EMD (server X) 4-3 which distributes the music content offered from the music offer firm X. Each EMD server 4 (4-1, 4-2, 4-3) provides for the personal computer 1 in which a user has the music content to which lineup was carried out original with each company through a network 2. Moreover, in each EMD server 4 (4-1, 4-2, 4-3), the music content is distributed with a method which the method of each company with original cipher system of a music content, format of use condition (Usage Rule) information, compression method of a music content, charging system of a music content, etc. is adopted, and is different, respectively.

[0171] In a personal computer 1, as application software for performing playback, management, etc. of a music content the application for playback (A) which performs purchase and management of a music content, and playback from EMD (server A) 4-1 - 311 -- the application for playback (B) which performs purchase and management of a music content, and playback from EMD (server B) 4-2 -- 312 -- a music content -- portable -- a device -- (-- A --) -- six - one -- transmitting -- a device driver -- (-- A --) -- 313 -- a music content -- portable -- a device -- (-- B --) -- six - two -- transmitting -- a device driver -- (-- B --) -- 314 -- installing -- having -- ****. In addition, the application 311, 312 for playback shown by this drawing 7 corresponds to the application program 115 for purchase and driver 117 which were shown by drawing 4.

[0172] Moreover, the comprehensive management unit (X) 315 which performs comprehensive management of all the music contents stored in HDD21 is installed in the personal computer 1. This comprehensive management unit (X) 315 is further constituted by the reception interface 316 for EMD, the transmitting interface 317 for EMD, and the driver 318 for PD.

[0173] moreover, portable here -- (Device A) 6-1 is equipment of the dedication corresponding to the music offer firm A, and it is portable -- (Device B) 6-2 are equipment of the dedication corresponding to the music offer firm B, and they are portable -- (Device X) 6-3 shall be equipment of the dedication corresponding to the music offer firm X. In addition, the music content stored in the memory card is enciphered with the original cipher system of each music offer firm, and formats of the compression method or use condition information also differ here. Therefore, direct continuation shall be carried out, for example to other device drivers etc., and a music content shall be transmitted no longer.

[0174] The application 311 for playback (A) performs processing which downloads the processing which uploads connection processing with an EMD server, a log file, etc., a music content, a contents key, use condition information, etc. This application 311 for

playback (A) performs connection processing only to a corresponding EMD server. Here, the application 311 for playback (A) cannot perform processing corresponding to EMD (server A) 4-1, and cannot perform connection processing to other EMD servers. moreover, the application 311 for playback (A) processing [authentication] and is [at the time of connecting with EMD (server A) 4-1] portable -- encryption/decryption processing of the music content stored in the authentication processing at the time of connecting with (Device A) 6-1 and HDD21 and use condition information etc. is performed. The application 311 for playback (A) enciphers the music content downloaded from EMD (server A) 4-1, and its use condition information with a contents key, enciphers this contents key with a session key, and stores it in HDD21. In addition, the respectively original method is used for the method of encryption processing with each application for playback. Therefore, if it is not the application for playback of dedication even if it is the music content stored in same HDD21 in a personal computer 1, a code can be decoded no longer in other applications for playback.

[0175] Moreover, the application 311 for playback (A) also performs management of the use condition information added to each music content. For example, the application 311 for playback (A) processes carrying out 1 batch decrement of the count limit value of playback or a duplicate, whenever it performs playback and reproduction, when the count limit value of playback is described by use condition information and the limit of the count of playback of contents is carried out etc.

[0176] Moreover, the application 311 for playback (A) transmits the music content and use condition information which self has managed on HDD21 to the reception interface 316 for EMD of the comprehension management unit (X) 315.

[0177] The application 312 for playback (B) performs processing which downloads the processing which uploads connection processing with an EMD server, a log file, etc., a music content, a contents key, use condition information, etc. This application 312 for playback (B) performs connection processing only to a corresponding EMD server. The application 312 for playback (B) cannot perform processing corresponding to EMD (server B) 4-2, and, specifically, cannot perform connection processing to other EMD servers. moreover, the application 312 for playback (B) processing [authentication] and is [at the time of connecting with EMD (server B) 4-2] portable -- encryption/decryption processing of the music content stored in the authentication processing at the time of connecting with (Device B) 6-2 and HDD21 and use condition information etc. is performed. The application 312 for playback (B) enciphers the music content downloaded from EMD (server B) 4-2, and its use condition information with a contents key, enciphers this contents key with a session key, and stores it in HDD21.

[0178] Moreover, the application 312 for playback (B) also performs management of the use condition information added to each music content. For example, the application 312 for playback (B) processes carrying out 1 batch decrement of the count limit value of playback or a duplicate, whenever it performs playback and reproduction, when the count limit value of playback is described by use condition information and the limit of the count of playback of contents is carried out etc.

[0179] Moreover, the application 312 for playback (B) transmits the music content and use condition information which self has managed on HDD21 to the reception interface 316 for EMD of the comprehension management unit (X) 315.

[0180] a device driver (A) 313 is portable -- it is the application software which performs a transfer of the music content of (Device A) 6-1 etc. a device driver (A) 313 is portable -
- a music content is transmitted to (Device A) 6-1.

[0181] a device driver (B) 314 is portable -- it is the application software which performs a transfer of the music content of (Device B) 6-2 etc. a device driver (B) 314 is portable -
- a music content is transmitted to (Device B) 6-2.

[0182] comprehension -- management -- a unit -- (-- X --) -- 315 -- EMD -- a server -- (-- X --) -- four - three -- from -- a music content -- offer -- winning popularity -- music -- offer -- a firm -- X -- dedication -- application software -- it is -- while -- a device driver -- (-- A --) -- 313 -- and -- a device driver -- (-- B --) -- 314 -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- between -- a music content -- and -- use -- conditions -- information -- a transfer -- carrying out -- a personal computer -- one -- inside -- a music content -- comprehensive -- management -
- carrying out -- management -- software -- it is also . moreover, the dedication which is the music regenerative apparatus of a pocket mold about the music content to which self manages is portable -- it can transmit to (Device X) 6-3.

[0183] In addition, this comprehension management unit (X) 115 performs processing corresponding to the contents manager 111 shown in drawing 4 . [0184] the interface module for connection with (Device X) 6-3 with the portable driver 318 for PD -- it is -- this -- portable -- the authentication processing and encryption processing between (Device X) 6-3 are performed. moreover -- PD -- ** -- a driver -- 318 -- others -- portable -- a device -- eight -- nine -- a music content -- etc. -- transmitting -- a case -- **** -- a device driver -- (-- A --) -- 313 -- a device driver -- (-- B --) -- 314 -- minding -- a music content and use condition information -- transmitting .

[0185] EMD -- ** -- reception -- an interface -- 316 -- playback -- ** -- application -- (-- A -) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- from -- a music content -- and -- use -- conditions -- information -- reception -- EMD -- a server -- (-- X --) -- four - three -- from -- a network -- two -- minding -- transmitting ---having had -- a music content -- and -- use -- conditions -- information -- reception -- and -- PD -- ** -- a driver - 318 -- between -- a music content -- and -- use -- conditions -- information -- transmission and reception -- carrying out .

[0186] EMD -- ** -- reception -- an interface -- 316 -- playback -- ** -- application -- (-- A -) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- from -- a music content -- and -- use -- conditions -- information -- receiving -- a case -- **** -- mutual recognition -- processing -- a cipher system -- conversion -- transmitting -- a music content -- adding -- having had -- use -- conditions -- information -- a format -- conversion -- transmitting -- a music content -- compression -- a method -- conversion -- etc. -- carrying out . a cipher system -- use -- conditions -- information -- compression -- a method -- conversion -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- using -- **** -- a method -- from -- comprehension -- management -- a unit -- (-- X --) -- 315 -- using -- **** -- a method -- changing -- having . The method which the comprehension management unit (X) 315 uses here is hereafter called a unification transfer protocol. and -- EMD -- ** -- reception -- an interface -- 316 -
- such -- unification -- a transfer protocol -- having changed -- a music content -- and -- use -- conditions -- information -- PD -- ** -- a driver -- 318 -- minding -- a device driver -- (-- A --) -- 313 -- a device driver -- (-- B --) -- 314 -- transmitting . moreover, the reception

interface 316 for EMD is portable through the driver 318 for PD in the music content and use condition information which were changed into the unification transfer protocol -- it transmits to (Device X) 6-3.

[0187] thus -- EMD -- a server -- (-- A --) -- four - one -- and -- EMD -- a server -- (-- B --) -- four - two -- from -- providing -- having -- a music content -- once -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- downloading -- having -- a music content -- a cipher system -- compression -- a method -- use -- conditions -- information -- unification -- a transfer protocol -- changing -- having -- comprehension -- management -- a unit -- (-- X --) -- 315 -- transmitting -- having . The comprehension management unit (X) 315 is manageable in generalization in the music content of EMD (server A) 4-1, an EMD server (B4 -2), and each contents offer firm that downloaded from EMD (server X) 4-3.

[0188] Moreover, the reception interface 316 for EMD has the function of the duplicate (copy) of a music content, migration (MUBU), check-in, and check-out.

[0189] EMD -- ** -- reception -- an interface -- 316 -- a user -- from -- a duplicate -- an instruction -- migration -- an instruction -- following -- for example, -- playback -- ** -- application -- (-- A --) -- 311 -- playback -- ** -- application -- (-- B --) -- 312 -- managing - - having -- **** -- a music content -- comprehension -- management -- a unit -- (-- X --) -- 315 -- a duplicate -- migration -- carrying out -- processing -- carrying out . In this case, the reception interface 316 for EMD changes a description format of the cipher system of a music content and a compression method, and use conditions, and let it be a unification transfer protocol.

[0190] Moreover, according to CD ripping instruction from a user, or a check-in instruction, processing which reproduces and checks in at the music content stored in external media and the portable devices 6 (6-1, 6-2, 6-3), such as a compact disk, at the comprehension management unit (X) 315 is performed. In this case, if the description format of the cipher system of a music content and a compression method, and use conditions is not made into the unification transfer protocol, the reception interface 316 for EMD performs these conversion, and let it be a unification transfer protocol.

[0191] moreover, portable in the music content managed by the comprehension management unit (X) 315 according to the check-out instruction from a user -- processing recorded on (Device X) 6-3 is performed. In this case, if the description format of the cipher system of a music content and a compression method, and use conditions is not made into the unification transfer protocol, the reception interface 316 for EMD performs these conversion, and let it be a unification transfer protocol. Moreover, 1 **** of the counts of use conditions which can be checked out is carried out in this case.

[0192] Moreover, in the comprehension management unit (X) 315, as shown in drawing 8 , a unification transfer protocol is formed in the lower layer of the application layer, and data transfer with other applications for playback is performed in this layer. And furthermore the comprehension management unit (X) 315 is this unification transfer protocol, it is performing data transmission and reception with EMD (server X) 4-3 by setting a lower layer to http (hyperText Transfer Protocol).

[0193] In the above music content distribution systems of a configuration, the comprehension management unit (X) 315 acquires the music content distributed from EMD (server A) 4-1 and EMD (server B) 4-2, and playback and management are

performed. and EMD (server X) 4-3 and the EMD server (A) 4 -- portable in the music content distributed from -1 and EMD (server B) 4-2 -- it can transmit now to (Device X) 6-3.

[0194] Thus, focusing on the comprehension management unit (X) 315, between each application for playback, and a device driver, conversion of the cipher system of the music content to transmit, conversion of a format of the use condition information added to the music content to transmit, and conversion of the compression method of the music content to transmit are performed, and a transfer of a music content is performed in a music content distribution system using a unification transfer protocol. therefore -- for example, the music content downloaded from EMD server B4 -2 with the application 312 for playback (B) in the music content list downloaded from EMD (server A) 4-1 with the application 311 for playback (A) can be transmitted to the comprehension management unit (X) 315. for this reason -- for example, portable in an artist's music content offered only from the music offer firm A -- it can transmit to (Device X) 6-3. namely, the music content of various methods stored in the hard disk of a personal computer 1 in this music content distribution system since the cipher system of a music content, a format of use condition information, the compression method of a music content, etc. are changed into a unification transfer protocol -- the comprehension management unit (X) 315 -- portable -- it is reproducible (Device X) 6-3. Especially, in a music content distribution system, the degree of freedom [music content / the] of handling can be enlarged, aiming at protection of the copyright of a music content, since a cipher system and use condition information are changed in the case of a transfer.

[0195] That is, in a music content distribution system, between the applications for playback which perform playback and control of a music content, conversion of a cipher system and use condition information is performed at least, and a transfer of a music content and use condition information is performed. By this, in a music content distribution system, even if two or more applications for playback exist, the music content stored in HDD21 in a personal computer 1 can be moved freely, and a unific music content can be managed. Moreover, since use condition information is also transmitted with a music content, use conditions do not overlap to one music content, and the copyright of a music content can also be protected certainly.

[0196] (3) use condition information (explanation of the use condition information that it is generally used), next, explain an example of a format of use condition information used for the application 311 for playback (A).

[0197] In the application 311 for playback (A), the use condition information described by the tabular format as shown in drawing 9 (a), for example is used.

[0198] In the left column of a table, the policy of use conditions is described in the direction of a train, and the concrete value of each policy is described by the right column. For example, the day (from) which can be playback started, a playback end date (to), the price (pay/play) to one playback, etc. are described as a policy. Such use condition information is in the condition added to each music content, as shown in drawing 9 (b), and it is distributed from EMD (server A) 4-1. The application 311 for playback (A) controls a music content according to the policy described and its value. For example, suppose that the prices [as opposed to / as opposed to / in the day (from) which can be playback started / use condition information / November 24, 99 and one playback in a playback end date (to)] (pay/play) are described to be yes / 10 yen on

October 25, 99. In this case, even if playback of that music content is enabled from October 25, 99 and there is a playback instruction from a user before it, it forbids playback. Moreover, if playback of the music content is enabled till November 24, 99 and it serves as it or later, it will eliminate the music content. Moreover, the music content keeps separately the count which it is set up so that 10 yen accounting may be performed at every one playback, for example, the user reproduced as log information, and performs accounting only for the count which viewed and listened to the log information to the user who uploaded, viewed and listened to EMD (server A) 4-1.

[0199] (Explanation of the use condition information that the comprehension management unit (X) 315 uses), below, the use condition information that the comprehension management unit (X) 315 uses is explained. The use condition information which gives explanation below is added to the music content downloaded from EMD (server X) 4-3, and in case the above-mentioned comprehension management unit (X) 315 controls the music content, it is used. moreover -- this -- use - conditions -- information -- playback -- ** -- application -- (-- A --) -- 311 -- comprehension -- management -- a unit -- (-- X --) -- 315 -- between -- and -- playback -- ** -- application -- (-- B --) -- 312 -- comprehension -- management -- a unit -- (-- X --) -- 315 -- between -- a music content -- a transfer -- carrying out -- the time -- unification -- a format -- ***** -- using -- having . Hereafter, this use condition information is called unification use condition information.

[0200] Unification use condition information consists of an index file 331, an automaton file 332, a parameter file 333, and a history file 334, as shown in drawing 10 . Each file is described in XML (eXtensible Markup Language) language.

[0201] The reference source of each file etc. is described by the index file 331.

[0202] As shown in drawing 11 , the certificate of attestation (Cert) 344 for verifying the signature (Sig) 343 of the automaton description section 341 use conditions were described to be with the automaton, the authorization code (MAC:Message Authentication Code) 342 with a contents key, and a contents provider, and this signature is added to the automaton file 332. Here, a contents provider's private key and public key which created KC and contents for the contents key are set to K-1E and K1E, respectively.

[0203] The operating state of a music content is described by Extended State Machine the automaton description section 341 was described to be in the tuple train.

[0204] The set of the operating state of a current music content is set to Q, and, specifically, Q' is expressed with the automaton description section 341 for the set of the operating state of the music content after it sets the set of the input symbol showing the event of a music content to sigma and it carries out a state transition as follows.

$Q' = \{d | d = \delta(q, \alpha) | q \in Q, \alpha \in \sigma, \text{ and } \delta: Q \times \sigma \rightarrow Q\}$

As shown in this formula, the set of condition Q' after carrying out a state transition is expressed as d. This d is defined by the function delta with Variables q and alpha. q shows one operating state in the set Q of the operating state of a music content. alpha shows one event in the set sigma of an event. And Function delta Q Reaches, is sigma Described, comes, and is the map to Q of a set.

[0205] and the above Q, sigma, and Q' -- being based -- every -- tuple -- $\{ \langle q, \alpha, d \rangle | q \in Q, \alpha \in \sigma \}$

It expresses by carrying out. In addition, $\langle q, \alpha, d \rangle$ show combination with the permutation of q , α , and d .

[0206] It reproduces and (Play) reproduces (copy), and pays to σ here, and events, such as the amount of money (pay Y), time (from YMD) which can be playback started, playback termination time (to YMD), usable days (in D days), and a null event (ϵ), are described as follows.

$\sigma = \{\text{Play, copy, pay } Y, \text{ from YMD, to YMD, in } D \text{ days, } \epsilon\}$

Thus, the automaton description section 341 is described as mentioned above.

[0207] The concrete example of description to this automaton description section 341 is explained.

[0208] For example, the example of description by the tuple train of the automaton in which transition of a music content as shown in drawing 12 of operation is shown is shown in drawing 13.

[0209] This automaton carries out a state transition which is explained below.

[0210] First, it changes in a condition q_1 and the condition q_5 from an initial state q_0 .

After a condition q_1 and a condition q_5 , it operates in parallel, respectively.

[0211] If the predetermined amount of money (for example, 10 yen) pays and an event (pay10) occurs in the condition q_1 , it will change to a condition q_2 . In the condition q_2 , if a play event (play) occurs, it will change to a condition q_1 . That is, with this automaton, if payment of 10 yen is carried out, it is shown that playback of a music content is attained only once. Moreover, if the predetermined amount of money (for example, 1000 yen) pays and an event (a. pay1000) occurs in the condition q_1 , it will change to a condition q_3 . In the condition q_3 , if a play event (play) occurs, it will change in this condition q_3 again. That is, with this automaton, if payment of 1000 yen is carried out, it is shown that a music content becomes a count reproducible without a limit. Moreover, if the n times as much amount of money as 1 time of the playback amount of money (for example, 10 yen) pays and an event (pay10 \times n) occurs in the condition q_1 , it will change to a condition q_4 . After changing to a condition q_4 , if a play event (play) occurs, it will change in this condition q_4 again. And in this condition q_4 , if n times of play events occur, it will change in the condition q_1 . That is, with this automaton, if payment of 10 \times n yen is carried out, it is shown that playback of a music content is attained n times.

[0212] Moreover, if the predetermined amount of money (for example, 100 yen) pays and an event (pay100) occurs in the condition q_5 , it will change to a condition q_6 . In the condition q_6 , if a copy event (copy) occurs, it will change to a condition q_5 . Moreover, in the condition q_6 , if a copy event (copy) occurs, it will change to a condition q_8 . In the condition q_8 , if a play event (play) occurs, it will change in this condition q_8 again. Moreover, in this condition q_8 , if a copy event (copy) occurs, it will change in the condition q_9 . It is in the termination condition that it changes to no condition and an event cannot be generated in the condition q_9 , either. That is, with this automaton, if payment of 100 yen is carried out, it is shown that a music content can be copied once to other devices. Moreover, with this automaton, although any number of times of reproducing the copied music content are possible, when it copies to other devices etc., it is shown that playback becomes impossible.

[0213] Moreover, if the predetermined amount of money (for example, 2000 yen) pays and an event (a. pay2000) occurs in the condition q_5 , it will change to a condition q_7 . In the condition q_7 , if a copy event (copy) occurs, it will change in this condition q_7 again.

Moreover, in the condition q7, if a copy event (copy) occurs, it will change to a condition q8. In the condition q8, if a play event (play) occurs, it will change in this condition q8 again. Moreover, in this condition q8, if a copy event (copy) occurs, it will change in the condition q9. It is in the termination condition that it changes to no condition and an event cannot be generated in the condition q9, either. That is, with this automaton, if payment of 2000 yen is carried out, it is shown that a music content can be copied to other devices without a count limit. Moreover, with this automaton, although any number of times of reproducing the copied music content are possible, when it copies to other devices etc., it is shown that playback becomes impossible.

[0214] And when a tuple train describes the automaton which carries out a state transition as mentioned above, it comes to be shown in drawing 13 .

[0215] Moreover, the automaton description section 341 may describe juxtaposition composition of operating state in order to update actuation of a music content. For example, juxtaposition composition with actuation a0 and actuation a1 is expressed with a tuple train as follows.

Action accompanying a state transition may be described in <q0, alpha, and a0.q0> <q0, alpha, a1.q0> and the automaton description section 341. For example, action is expressed with tuple as follows.

<q0, alpha, q1;action> This action is expressed as a function using the variable defined beforehand. Moreover, a variable consists of ID, a scope, and initial value. There are classes, such as the music content, an album, and the whole system, in a scope. For example, the variable showing the price of acquisition of an album (a) is set to n, and is described like a.n:=1000. Thus, an example of the automaton description section 341 action to a variable was described to be is shown below.

<q0, pay100, q1, a.n:=a.n-100> ... (1)

<q0, pay (a. n), q1, a.n:=0> ... (2)

<q1, play, q2> ... (3)

This example shows that the acquisition price {a formula (1)} of one music content affects the price of album acquisition {a formula (2)}.

[0216] The above automaton description sections 341 consist of an entry ID 345, content ID 346, version information 347, variable information 348, and a tuple train 349, as shown in drawing 14 .

[0217] The example of the automaton description section 341 in which the description format was defined as mentioned above is explained.

[0218] In addition, the event and command which are used for below by description of an automaton are defined by DTD (Document Type Definition) specified based on the specification of XML. For example, as shown in drawing 15 , a playback actuation (play), duplicate actuation (copy), right purchase (pay-for-play) of playback, right-of-reproduction-copyright purchase (pay-for-copy), right purchase (pay-for-album-play) of album playback, album right-of-reproduction-copyright purchase (pay-for-album-copy), usable opening day (from), and use end date (to) and the Nur actuation (null) are defined by DTD as an event.

[0219] Drawing 16 is the example of description of the automaton description section 341 by the XML language which shows that a music content can be reproduced from September 1, 1999.

[0220] The description shown in this drawing 16 serves as an automaton as shown in drawing 17 . This automaton consists of a condition q1 of an initial state, and a condition q2. In the condition q1, if the date is set to September 1, 1999 of an usable opening day (from), it will change to a condition q2. And in the condition q2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Thus, this automaton is controlled to enable September 1, 1999 to playback for a music content.

[0221] Drawing 18 is the example of description of the automaton description section 341 by the XML language which shows that a music content can be reproduced till October 31, 1999.

[0222] The description shown in this drawing 18 serves as an automaton as shown in drawing 19 . This automaton consists of a condition q1 of an initial state, and a condition end of a termination condition. In the condition 2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Moreover, in the condition 2, if October 31, 1999 of a use end date (to) comes, it will change to Condition end. When it comes to Condition end, it changes to no condition and an event is not generated, either. Thus, this automaton is controlled to make playback possible for a music content till October 31, 1999.

[0223] Drawing 20 is the example of description of the automaton description section 341 by the XML language which shows that the refreshable period of a music content is from September 1, 1999 to October 31, 1999, and the count of refreshable is 16 times.

[0224] The description shown in this drawing 20 serves as an automaton as shown in drawing 21 . This automaton consists of a condition q1 of an initial state, a condition q2, and a condition end of a termination condition. In the condition q1, if September 1, 1999 of an usable opening day (from) comes, it will change to a condition q2. And in the condition q2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Moreover, if October 31, 1999 of a use end date (to) comes or a playback event (playx16) occurs 16 times in the condition 2, it will change to Condition end. When it comes to Condition end, it changes to no condition and an event is not generated, either. Thus, this automaton carries out the playback period of a music content to from September 1, 1999 to October 31, 1999, and is controlling that count of playback to 16 times.

[0225] Drawing 22 is the example of description of the automaton description section 341 by the XML language which shows that the count of playback of a music content is restricted to 16 times.

[0226] Next, as shown in drawing 23 , the certificate of attestation 354 for verifying the signature 353 of the parameter description section 351, the authorization code 352 with a contents key, and a contents provider and this signature is added to the parameter file 333. Here, a contents provider's private key and public key which created KC and contents for the contents key are set to K-1E and K1E, respectively.

[0227] Moreover, a parameter file 333 can be rewritten by the contents provider (for example, secondary providers, such as a contents retailer and a contents middle contractor) other than the contents provider who created the above-mentioned automaton file 332. As the rewritten parameter file 333 is shown in drawing 24 , the unique entity ID 55 given to each provider, middle contractor, etc. is added. Here, K'C is a secondary provider's contents key and serves as $K'C=H(KC, \text{EntityID})$. In addition, H

is an one-way hash function here. A secondary provider's contents key K'C is created from a primary provider's contents key KC. A primary provider and a secondary provider are distinguished with the certificate of attestation.

[0228] If the contents key is obtained, when MAC will perform and a contents key will not be obtained by the reasons of safety etc. as an approach of verifying a parameter file 333, it verifies with a signature and a certificate.

[0229] The protocol verified by MAC is as follows. S and a secondary provider are set to A and a terminal is set to B for the primary provider of contents. S->A shows transmission to A from S, S->B shows transmission to B from S, and A->B shows transmission to B from A. Moreover, IDA shows ID of Device A.

[0230] S->A: K'C=H (KC, IDA)

S->B: X=EKs (KC)

A->B: IDA, Parameters, M=MACK'C (Parameters)

B: M MACK'c (Parameters).

The multiplier of the function for modification of the value described by the automaton section 41 of the above-mentioned automaton file 31 is described by this parameter description section 351. For example, in the example shown in drawing 13, the price of a music content may serve as a function as follows in the automaton section 41, for example.

< -- q0, pay (f1 (10)), and q1> <q1, pay (f2 (10) xn), q2> -- this case -- the above-mentioned functions f1 and f2 -- for example, it sets as follows.

$f1(n) = 0.9nf2(n) =$ -- by defining $90 + 0.1n$ of functions in this way, for example, a primary provider defines the default of a price, and a secondary provider can rewrite a parameter file 333 and can change a price.

[0231] The above parameter description sections 351 consist of an entry ID 356, content ID 357, and multiplier information 358, as shown in drawing 25.

[0232] A history file 334 is a file which describes the locus of actuation of the music content which operates based on the contents of description in the automaton description section 341. The status and the variable in tuple of the above-mentioned automaton description 41 are recorded on this history file 334. For example, when playback is performed twice to drawing 13 mentioned above in an example, it is set to <q0, q1, q0, q1>, and, thereby, the locus of the following actuation can be obtained. <pay10, play, pay10, play> If this is totaled, for example, upload etc. is carried out to the comprehension management unit (X) 315, a user can pay and the amount of money can be calculated.

[0233] As mentioned above, in a music content distribution system, since the automaton which programmed the policy itself and its concrete value has described use condition information, the degree of freedom of a publication of the use conditions of contents can be raised.

[0234] (4) restoration of the destroyed music content, and re-download -- next, explain backup of the music content by the comprehension management unit (X) 315.

[0235] First, the key management method of the music content of the comprehension management unit (X) 315 is explained using drawing 26.

[0236] The comprehension management units (X) 315 are music contents C1, C2, and C3 to HDD21 in a personal computer 1... Cn is stored. Moreover, the comprehension management units (X) 315 are each music contents C1, C2, and C3... They are the

contents keys Kc1, Kc2, and Kc3 corresponding to Cn... Kcn is also stored. The contents key Kc serves as relation of one to one to music content C. Moreover, each music contents C1, C2, and C3 ... The content ID for [each] identifying is added to Cn. It is this content ID CID1, CID2, and CID3 ... It is referred to as CIDn.

[0237] Music contents C1, C2, and C3 ... Cn is the contents keys Kc1, Kc2, and Kc3... It is enciphered by Kcn and they are E (Kc1, C1), E (Kc2, C2), and E (Kc3, C3)... It is recorded in HDD21 of a personal computer 1 in the condition of having been referred to as E (Kcn, Cn). Here, E (K, C) shows that Contents C are enciphered with Key K.

Usually, content ID is made into the condition that it is recorded on the header of music content C etc., and is enciphered with music content C, or MAC was added to music content C, and separation has become impossible with the music content body.

[0238] Moreover, contents keys Kc1, Kc2, and Kc3 ... It is enciphered with the storage key KS and Kcn is E (KS, Kc1), E (KS, Kc2), and E (KS, Kc3)... It is recorded on HDD21 of a personal computer 1 in the condition of having been referred to as E (KS, Kcn).

This storage key KS has the so-called Tampa-proof nature, and is saved from the regular user in the record section which cannot be referred to.

[0239] In the comprehension management unit (X) 315 to which key management is performed as mentioned above, in reproducing a music content C1, the code of the contents key Kc1 is canceled using the storage key KS, then it cancels the code of a music content C1 using this contents key Kc1, for example. By this, the comprehension management unit (X) 315 can reproduce a music content C1.

[0240] moreover, in the comprehension management unit (X) 315 to which key management is performed as mentioned above for example, portable [from HDD21] in a music content C1, in moving to (Device X) 6-3 (MOVE) Portable device (X) If mutual recognition is performed among 6-3 and authentication is completed, the code of the contents key Kc1 will be canceled using the storage key KS. then, the contents key Kc1 is enciphered with a session key, and portable in the enciphered contents key Kc1 and the enciphered music content C1 -- it transmits to (Device X) 6-3. And elimination is carried out for both the music contents C1 to the contents key Kc1 from HDD21. by this, the comprehension management unit (X) 315 is portable in a music content C1 -- it can move to (Device X) 6-3.

[0241] Below, when HDD21 breaks, the restoration approach of a music content when it becomes impossible to reproduce a music content and a contents key from HDD21 is explained.

[0242] First, the comprehension management unit (X) 315 usually sometimes saves the backup data of enciphered music content C and the contents key Kc at the inside of HDD21, other record media, etc.

[0243] Moreover, the comprehension management unit (X) 315 usually sometimes manages the record of purchase of a music content downloaded from -3, and the list of the content ID of all the music contents memorized in EMD (server X) 4HDD21 as use log information. this log information is portable when a music content is downloaded from EMD (server X) 4-3 -- it is made to update when music contents, such as migration to (Device X) 6-3, are controlled Moreover, log information is stored in another field and other record media of HDD21. The comprehension management unit (X) 315 uploads this log information to EMD (server X) 4-3, periodical or whenever it accessed.

[0244] And when music content C and the contents key Kc which are stored in HDD21 of the comprehension management unit (X) 315 have been destroyed, processing as shown below is performed.

[0245] When music content C and the contents key Kc have been destroyed, first, the comprehension management unit (X) 315 accesses EMD (server X) 4-3, and performs user authentication.

[0246] Then, EMD (server X) 4-3 generate the adjustment verification value ICV (Integrity Check Value) from a user's attested user ID with reference to the use log information of the comprehension management unit (X) 315. This adjustment verification value ICV is generated as follows based on CID which is the content ID of music content C described by use log information, and the storage key KS of the comprehension management unit (X) 315. $ICV = H(KS, CID1 || CID2 || \dots || CIDn)$ -- here, $H(K, Data)$ is an one-way hash function, and the value changes with keys K.

[0247] Then, EMD (server X) 4-3 transmit the generated adjustment verification value ICV to the comprehension management unit (X) 315.

[0248] Then, if music content C or the contents key Kc is backed up, the comprehension management unit (X) 315 restores the backup data, and saves music content C or the contents key Kc in HDD21. Moreover, if music content C or the contents key Kc is not backed up, I have music content C or the contents key Kc destroyed from EMD (server X) 4-3 re-distributed. Accounting will not be performed if EMD (server X) 4-3 are contents purchased with reference to a user's purchase hysteresis before at this time.

[0249] The comprehension management unit (X) 315 performs the above processing, and revives destroyed music content C or the contents key Kc.

[0250] And the comprehension management unit (X) 315 checks CID of the music content with the above-mentioned adjustment verification value ICV, when performing playback and control of revitalized music content C or the contents key Kc. Thus, by checking music content C or the contents key Kc revived using the adjustment verification value ICV for example, portable in a certain music content Ci -- from HDD21, by moving to (Device X) 6-3, when eliminated Even if it keeps in mind $E(Kci, Ci)$ which is the music content Ci as which the malicious user was enciphered and restores, that those data are reproduced cannot control migration etc., either.

[0251] In addition, when music content C and not the contents key Kc but the storage key KS is destroyed, re-install of the comprehension management unit (X) 315 is performed. If log information is uploaded while carrying out user registration to EMD (server X) 4-3 even if it is this case, restoration and re-download can be carried out by the approach mentioned above.

[0252] Thus, it can restore in a music content distribution system, protecting copyright by crash of a hard disk etc., for example, even if it is the case where the music content has been destroyed. For example, if the music content purchases to normal, it can be made to revive for nothing.

[0253] (5) comprehension -- management -- a unit -- a master -- a key -- and -- authentication -- a key -- etc. -- distribution -- an approach -- comprehension -- management -- a unit -- (-- X --) -- 315 -- portable -- a device -- (-- X --) -- six - three -- between -- **** -- portable -- a device -- (-- X --) -- six - three -- a proper -- ID -- and -- authentication -- a key (MG-ID/IK) -- comprehension -- management -- a unit -- (-- X --) -

- 315 -- a proper -- a master -- a key (OMG-MK) -- using -- mutual recognition -- carrying out -- having .

[0254] as portable as the comprehension management unit (X) 315 -- portable [from the comprehension management unit (X) 315] among (Device X) 6-3, when mutual recognition is performed -- portable in transmitting a music content to (Device X) 6-3 (check-out) -- the music content from (Device X) 6-3 to the comprehension management unit (X) 315 can be returned now (check-in). in addition, the comprehension management unit (X) 315 saves the music content enciphered in HDD21 of a personal computer 1, and is portable -- (Device X) 6-3 save the music content enciphered to storages, such as an internal memory card. therefore, portable from the comprehension management unit (X) 315 -- when transmitting a music content to (Device X) 6-3, the music content on HDD21 of a personal computer 1 is portable -- it will be transmitted on the memory card with which (Device X) 6-3 were equipped. moreover, portable -- portable, when transmitting a music content to the comprehension management unit (X) 315 from (Device X) 6-3 -- the music content on the memory card with which (Device X) 6-3 were equipped will be transmitted on HDD21 of a personal computer 1.

[0255] Portable device (X) 6-3 has held beforehand ID information (MG-ID), the authentication key (MG-IK) for two or more generations, and the master key (OMG-MK) for two or more generations from the time of factory shipments. Portable device (X) 6-3 These keys etc. are not behind supplied to 6-3 from the exterior. Portable device (X) 6-3 updates the generation of an authentication key (MG-IK) and a master key (OMG-MK) if needed. Portable device (X) 6-3 performs mutual recognition with the newest generation's authentication key and master key by which renewal of a generation was carried out, and does not perform mutual recognition with an old generation's authentication key and master key. hereafter, portable -- (Device X) 6-3 shall hold the authentication key (MG-IK [0-99]) and master key (OMG-MK [0-99]) for 100 generations of the 0th generation to the 99th generation In addition, the authentication key of the i-th generation is indicated to be (MG-IK [i]), and the master key of the i-th generation is indicated to be (OMG-MK [i]).

[0256] Moreover, the comprehension management unit (X) 315 can transmit and save a music content in a personal computer 1 from the compact disk for audios etc. by holding a master key (OMG-MK). Moreover, by holding a master key (OMG-MK), the comprehension management unit (X) 315 can download a music content from EMD (server X) 4-3, and can save it in a personal computer 1.

[0257] Here, in the comprehension management unit (X) 315, although a music content can be transmitted from a compact disk, it is that from which the master key (OMG-MK) which can transmit a music content also from EMD (server X) 4-3 differed also from the master key (OMG-MK) which cannot download a music content, and the compact disk from EMD (server X) 4-3. Hereafter, although a music content can be transmitted from a compact disk, from EMD (server X) 4-3, the thing of the key which cannot download a music content is also called key only for ripping, and the thing of a key which can transmit a music content also from EMD (server X) 4-3 is also called EMD key also from a compact disk.

[0258] In addition, in this example, the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, and the master key after the 1st generation (OMG-MK [1-99]) is an EMD key.

[0259] Below, the procedure of processing in which the key only for ripping was used is explained.

[0260] portable in CD-ROM361 in which the install software of the comprehension management unit (X) 315 was stored, as shown in drawing 27 , when the comprehension management unit (X) 315 is installed from CD-ROM -- (Device X) 6-3 and the floppy (trademark) disk 362 are sold by the set. portable in a floppy disk 362 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK [0]) of the 0th generation are stored.

[0261] Then, in order to make usable the sold portable (device X) 6-3 grade, a personal computer 1 is first equipped with CD-ROM361 (step S11). Then, the comprehension management unit (X) 315 is installed in a personal computer 1 from this CD-ROM361 (step S12). Then, the comprehension management unit (X) 315 will be stored in the hard disk of a personal computer 1 (step S13). then, it is stored in the floppy disk 362 -- portable -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK[0]) of the 0th generation are saved in a personal computer 1 (step S14).

[0262] By this, the comprehension management unit (X) 315 can store now the music content offered by music CD363 grade in the hard disk of a personal computer 1 (step S15). In addition, since the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, it can download a music content no longer from EMD (server X) 4-3.

[0263] moreover, portable -- although (Device X) 6-3 hold the authentication key and master key for 100 generations with which renewal of a generation is carried out inside, they are made into the 0th generation in the state of initialization. for this reason, as portable as the comprehension management unit (X) 315 holding the authentication key of the 0th generation, and a master key -- the mutual recognition of (Device X) 6-3 becomes possible. therefore, portable in the music content offered by music CD363 grade -- it can store now in the memory card of (Device X) 6-3 (step S16).

[0264] portable, as it is shown in drawing 28 on the other hand, when the comprehension management unit (X) 315 is offered through a network -- the address, user ID, a password, etc. of the EMD registration server 3 on the Internet are offered with (Device X) 6-3.

[0265] Then, in order to make usable the sold portable (device X) 6-3 grade, the EMD registration server 3 on a network is first accessed using user ID and a password (step S21). Then, the EMD registration server 3 performs authentication of user ID and a password (step S22). then, if there is no problem in authentication, the EMD registration server 3 is as portable as the install software of the comprehension management unit (X) 315 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK [0]) of the 0th generation are transmitted to a personal computer 1 (step S23). then, a personal computer 1 is portable while it starts the install software of the comprehension management unit (X) 315 and installs the comprehension management unit (X) 315 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the

master key (OMG-MK [0]) of the 0th generation are saved at HDD21 (step S24). Then, the comprehension management unit (X) 315 will be stored in a hard disk (step S25).

[0266] By this, the comprehension management unit (X) 315 can store now the music content offered by music CD363 grade in HDD21 of a personal computer 1 (step S26). In addition, since the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, it can download a music content no longer from EMD (server X) 4-3.

[0267] moreover, portable -- although (Device X) 6-3 hold the authentication key and master key for 100 generations with which renewal of a generation is carried out inside, they are made into the 0th generation in the state of initialization. for this reason, as portable as the comprehension management unit (X) 315 holding the authentication key of the 0th generation, and a master key -- the mutual recognition of (Device X) 6-3 becomes possible. therefore, portable in the music content offered by music CD363 grade -- it can store now in the memory card of (Device X) 6-3 (step S27).

[0268] In addition, it is not restricted to the approach shown in the above drawing 27 and drawing 28 , but the comprehension management unit (X) 315 and the master key of the 0th generation only for ripping (OMG-MK [0]) are stored in CD-ROM361, and portable ID for authentication with (Device X) 6-3 and the authentication key (MG-ID/IK) of the 0th generation may be offered through a network.

[0269] Below, the key only for ripping is updated in an EMD lock at a key, and the procedure of processing of enabling it to deal with the music content downloaded from EMD (server X) 4-3 is explained.

[0270] By the procedure shown in drawing 27 or drawing 28 , the comprehension management unit (X) 315 is offered through networks, such as removable media, such as CD-ROM, and the Internet, and is installed in HDD21 in a personal computer 1. at this time, the comprehension management unit (X) 315 holds the master key (OMG-MK [0]) of the 0th generation which is exclusively for ripping, and ID for authentication and the authentication key (MG-ID/IK [0]) of the 0th generation, and is portable -- he is also the generation of the key of (Device X) 6-3 in the default state.

[0271] First, a personal computer 1 accesses the EMD registration server 3 on a network using user ID and a password, as shown in drawing 29 (step S31). Then, the EMD registration server 3 performs authentication of user ID and a password (step S32). Then, if there is no problem in authentication, the EMD registration server 3 will register ID information (OMG-ID) on a personal computer 1, and will generate the certificate of attestation (Cert [PK]) of a public key (OMG-PK) for the comprehension management unit (X) 315 to connect with EMD (server X) 4-3, a private key (OMG-KS), and a public key (step S33). Then, the EMD registration server 3 transmits the certificate of attestation (Cert [PK]) of the generated public key (OMG-PK), a private key (OMG-KS), and a public key to a personal computer 1 (step S34).

[0272] then, the EMD registration server 3 is portable -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [i]) of the i-th generation, and the master key (OMG-MK [i]) of the i-th generation are transmitted to a personal computer 1 (step S35). Then, the comprehension management unit (X) 315 of a personal computer 1 carries out renewal of a generation of these keys at the i-th generation based on received ID information (MG-ID), the authentication key (MG-IK [i]) of the i-th generation, and the master key (OMG-MK [i]) of the i-th generation (step S36). then, the comprehension management unit (X) 315 is portable -- it attests among (Device X) 6-3

(step S37). Portable device (X) 6-3 will update the generation of a self key to the i-th generation, if authentication is carried out (step S38).

[0273] By this, the comprehension management unit (X) 315 can store in HDD21 of a personal computer 1 the music content which carried out the Dow-Jones load from EMD (server X) 4-3 while being able to store the music content offered by music CD363 grade in the hard disk of a personal computer 1.

[0274] Below, the procedure which carries out renewal of a generation of an EMD key etc. is explained.

[0275] the comprehension management unit (X) 315 holds the master key (OMG-MK[i]) of the i-th generation, and ID for authentication and the authentication key (MG-ID/IK [i]) of the 0th generation, and is portable -- the generation of the key of (Device X) 6-3 is also the i-th generation.

[0276] First, if the EMD registration server 3 is accessed since a personal computer 1 is a certain processing as shown in drawing 30, the EMD registration server 3 will attest ID of the comprehension management unit (X) 315, and will transmit a ** (i+k) generation's authentication key (MG-IK [i+k]), and a ** (i+k) generation's master key (OMG-MK [i+k]) to a personal computer 1 (step S41). Then, the comprehension management unit (X) 315 of a personal computer 1 updates the authentication key and master key which were received in a ** (i+k) generation (step S42). then, the comprehension management unit (X) 315 is portable -- (Device X) 6-3 and authentication are performed (step S43). Portable device (X) 6-3 will update the generation of a self key in a ** (i+k) generation from the i-th generation, if authentication is carried out (step S44).

[0277] moreover, portable on the other hand, as shown in drawing 31 -- portable, when the generation of the authentication key which (Device X) 6-3 use is a ** (i+k) generation and the generation of the authentication key which the comprehension management unit (X) 315 holds is the i-th generation -- it will become authentication failure if authentication with (Device X) 6-3 and the comprehension management unit (X) 315 is performed (step S51). If authentication goes wrong, the comprehension management unit (X) 315 will perform a key demand to the EMD registration server 3 (step S52). If there is a key demand, the EMD registration server 3 will attest ID of the comprehension management unit (X) 315, and will transmit a ** (i+k) generation's authentication key (MG-IK [i+k]), and a ** (i+k) generation's master key (OMG-MK [i+k]) (step S53). Then, the comprehension management unit (X) 315 updates the authentication key and master key which were received in a ** (i+k) generation (step S54). then, the comprehension management unit (X) 315 is portable -- (Device X) 6-3 and authentication are performed (step S55).

[0278] By this, the comprehension management unit (X) 315 can store in HDD21 of a personal computer 1 the music content downloaded from EMD (server X) 4-3 while being able to store the music content offered by music CD363 grade in the hard disk of a personal computer 1 (step S38).

[0279] as mentioned above -- a music content distribution system -- the comprehension management unit (X) 315 -- and portable -- he divides into the key and server connection key only for ripping the master key and authentication key which (Device X) 6-3 use, and is trying to download a server connection key through a network further For this reason, in a music content distribution system, even if the safety of the music

content distributed from the server increases, for example, the key only for ripping is torn, the music content downloaded from a server cannot be broken.

[0280] moreover -- a music content distribution system -- the comprehension management unit (X) 315 -- and portable -- renewal of a generation is carried out and the master key and authentication key which (Device X) 6-3 use are used. Furthermore, a master key and an authentication key are supplied through a network, and the comprehension management unit (X) 315 performs renewal of a generation. For this reason, the safety of a music content increases.

[0281]

[Effect of the Invention] According to this invention, a data processor performs playback and/or control of restoration of backup, or the re-distributed contents data based on the use log information re-acquired from the contents server.

[0282] By this, the contents data which carried out contents distribution through the network can restore contents data by this invention, aiming at protection of copyright, even if it is the case where it has once been destroyed.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the music content distribution structure of a system of the gestalt of operation of this invention.

[Drawing 2] It is drawing showing the configuration of the personal computer in the above-mentioned music content distribution system.

[Drawing 3] It is drawing showing the configuration of the portable device in the above-mentioned music content distribution system.

[Drawing 4] It is drawing explaining the function of the above-mentioned personal computer.

[Drawing 5] It is drawing showing an example of a display operator guidance window.

[Drawing 6] A sound recording program is drawing showing the example of a display displayed on a display.

[Drawing 7] It is drawing for explaining the unific handling of the contents from which a format differs for every distribution contractor in the above-mentioned music content distribution system.

[Drawing 8] It is drawing explaining the relation between a unification transfer protocol layer and an application layer.

[Drawing 9] It is drawing explaining a format of the use condition information that it is generally used.

[Drawing 10] It is drawing explaining the file which constitutes the unification use condition information that it is used in a comprehension management unit.

[Drawing 11] It is drawing explaining the configuration of the automaton file of the above-mentioned unification use condition information.

[Drawing 12] It is drawing explaining an example of the automaton in which transition of the music content described by the automaton description section of the above-mentioned automaton file of operation is shown.

[Drawing 13] It is drawing which expressed the above-mentioned automaton in the tuple train.

[Drawing 14] It is drawing explaining the configuration of the above-mentioned automaton description section.

[Drawing 15] It is drawing showing the event defined by DTD specified based on the specification of XML, and a command.

[Drawing 16] It is drawing showing the 1st example of description of the above-mentioned automaton description section.

[Drawing 17] It is the state transition diagram of the example of description of the above 1st.

[Drawing 18] It is drawing showing the 2nd example of description of the above-mentioned automaton description section.

[Drawing 19] It is the state transition diagram of the example of description of the above 2nd.

[Drawing 20] It is drawing showing the 3rd example of description of the above-mentioned automaton description section.

[Drawing 21] It is the state transition diagram of the example of description of the above 3rd.

[Drawing 22] It is drawing showing the 4th example of description of the above-mentioned automaton description section.

[Drawing 23] It is drawing explaining the configuration of the parameter file of the above-mentioned unification use condition information.

[Drawing 24] It is drawing explaining the configuration at the time of updating the above-mentioned parameter file.

[Drawing 25] It is drawing explaining the configuration of the parameter description section of the above-mentioned parameter file.

[Drawing 26] It is drawing explaining the management method of the contents by the above-mentioned comprehension management unit.

[Drawing 27] It is drawing explaining procedure in case a comprehension management unit is installed from CD-ROM.

[Drawing 28] It is drawing explaining procedure in case a comprehension management unit downloads and is installed from a network.

[Drawing 29] It is drawing explaining the update procedure updated in an EMD lock from a ripping key.

[Drawing 30] It is drawing explaining the 1st example of the procedure which updates an EMD key.

[Drawing 31] It is drawing explaining the 2nd example of the procedure which updates an EMD key.

[Description of Notations]

1 Personal Computer, 2 Network, 3 EMD Registration Server, 4 EMD Server, 6 Portable Device, 7 USB Interface, 21 Hard Disks, 311,312 Application for Playback, 313,314 Device Drivers, 315 Comprehension Management Unit, 316 Reception Interface for EMD, 317 Transmitting Interface for EMD, 318 PD Driver